目　录

第一章　交换环和它的某些性质

我们假定读者在近世代数课程中已经学过环的基本知识，如环的定义，子环，理想，商环，环的同态和同构，环的同态基本定理，环的直和，中国剩余定理，多项式环，主理想环以及唯一因子分解整环等等，在这一章里我们简要地介绍交换环的某些性质，其目的主要是明确我们在本书中采用的一些术语，同时也介绍某些新知识（素理想和极大理想，理想的扩张和限制，环的大根与小根等）.

如不声明，本书中的环均指是具有幺元素的交换环.

§1.1　理想的运算

设 $\mathfrak{a}$ 和 $\mathfrak{b}$ 是环 R 的理想，则

$$\mathfrak{a}+\mathfrak{b}=\{a+b\mid a\in\mathfrak{a},b\in\mathfrak{b}\}$$

也是环 R 的理想，叫作是理想 $\mathfrak{a}$ 和 $\mathfrak{b}$ 的**和**. 这也是环 R 中同时包含 $\mathfrak{a}$ 和 $\mathfrak{b}$ 的最小理想. 如果 $\mathfrak{a}+\mathfrak{b}=R$，则称理想 $\mathfrak{a}$ 与 $\mathfrak{b}$ **互素**. 类似地，对于环 R 的任意一个理想族 $\mathfrak{a}_i(i\in I)$，其中 I 可以是有限或无限集合，则定义它们的和为

$$\sum_{i\in I}\mathfrak{a}_i=\left\{\sum_{i\in I}a_i\mid a_i\in\mathfrak{a}_i(i\in I)\text{，并且只有有限个 }a_i\neq 0\right\}.$$

这是环 R 中包含所有 $\mathfrak{a}_i(i\in I)$的最小理想.

另一方面，对于环 R 的任意理想族 $\mathfrak{a}_i(i\in I)$，它们的（集合论的）交 $\bigcap_{i\in I}\mathfrak{a}_i$ 是 R 的理想，叫作是诸理想 $\mathfrak{a}_i(i\in I)$的**交**. 它显然是包含在每个理想 $\mathfrak{a}_i(i\in I)$之中的最大理想.

设 $\mathfrak{a}$ 和 $\mathfrak{b}$ 是环 R 的两个理想，集合

$$\mathfrak{ab}=\left\{\text{有限和}\sum_i a_ib_i\mid a_i\in\mathfrak{a},b_i\in\mathfrak{b}\right\}$$

也是环 R 的理想,叫作是理想 $\mathfrak{a}$ 与 $\mathfrak{b}$ 的积. 由于 R 是交换环,容易推得理想的积运算满足交换律,即 $\mathfrak{a}\mathfrak{b}=\mathfrak{b}\mathfrak{a}$. 并且,任意有限多个理想 $\mathfrak{a}_1,\mathfrak{a}_2,\cdots,\mathfrak{a}_n$ 的乘积是

$$\mathfrak{a}_1\mathfrak{a}_2\cdots\mathfrak{a}_n=\left\{\text{有限和}\sum_i a_{1i}a_{2i}\cdots a_{ni}\,\middle|\,a_{ji}\in\mathfrak{a}_j(1\leqslant j\leqslant n)\right\}.$$

特别地,对于理想 $\mathfrak{a}$ 可以定义它的幂 $\mathfrak{a}^n=\mathfrak{a}\mathfrak{a}\cdots\mathfrak{a}$($n$ 个),而规定 $\mathfrak{a}^0=R$.

易知 $\mathfrak{a}\mathfrak{b}\subseteq\mathfrak{a}\cap\mathfrak{b}$,但是反过来则不一定成立(见习题 5).

设 $\mathfrak{a}$ 和 $\mathfrak{b}$ 是环 R 的两个理想,定义 $\mathfrak{a}$ 对于 $\mathfrak{b}$ 的商为

$$(\mathfrak{a}:\mathfrak{b})=\{x\in R\mid x\mathfrak{b}\subseteq\mathfrak{a}\},$$

其中 $x\mathfrak{b}=\{xb\mid b\in\mathfrak{b}\}$. 易知$(\mathfrak{a}:\mathfrak{b})$是 R 的理想,而当 $\mathfrak{a}$ 或 $\mathfrak{b}$ 是主理想时,即 $\mathfrak{a}=(a)=aR,\mathfrak{b}=(b)=bR(a,b\in R)$时,我们也记成

$$(a:\mathfrak{b})=((a):\mathfrak{b}),\quad(\mathfrak{a}:b)=(\mathfrak{a}:(b)).$$

特别地,

$$(0:\mathfrak{b})=\{x\in R\mid x\mathfrak{b}=(0)\}=\{x\in R\mid bx=0,\text{对每个 }b\in\mathfrak{b}\}.$$

我们把$(0:\mathfrak{b})$叫作是 $\mathfrak{b}$ 的**零化理想**,并且表示成 $\mathrm{Ann}(\mathfrak{b})$. 而对环 R 中的每个元素 a,a 的零化理想即指为主理想$(a)=aR$ 的零化理想,记成 $\mathrm{Ann}(a)$. 于是

$$\mathrm{Ann}(a)=(0:a)=\{x\in R\mid xa=0\}.$$

如果 $\mathrm{Ann}(a)\neq(0)$,我们称 a 是环 R 中的一个**零因子**. 换句话说,a 是环 R 的零因子,当且仅当存在 R 中非零元素 b,使得 $ab=0$.对于每个非零环 R(即 $R\neq(0)$),0 显然是一个零因子,如果环 $R\neq(0)$并且没有 0 以外的零因子,我们便称 R 是一个**整环**.

以上我们介绍的理想之间的运算(和,交,积,商)均是同一个环 R 内理想之间的运算. 现在谈不同环中理想之间的运算:理想的扩张和限制. 设 A 和 B 是两个环,$f:A\to B$ 是环的同态. 如果 $\mathfrak{a}$ 为 A 的理想,则集合 $f(\mathfrak{a})$一般不必为 B 的理想(试举一例). 我们把 $f(\mathfrak{a})$在 B 中所生成的理想

$$f(\mathfrak{a})B=\left\{\text{有限和}\sum_i x_i y_i \;\middle|\; x_i\in f(\mathfrak{a}),y_i\in B\right\}$$

叫作是 A 中理想 $\mathfrak{a}$（通过同态 f）到环 B 中的**扩张**. 或者叫作是 $\mathfrak{a}$ 在 B 中的**扩张理想**，表示成 $\mathfrak{a}^e$. 另一方面，如果 $\mathfrak{b}$ 是环 B 的理想，则

$$f^{-1}(\mathfrak{b})=\{a\in A\,|\,f(a)\in\mathfrak{b}\}$$

必然是环 A 的理想（试证明之），称作是环 B 中理想 $\mathfrak{b}$（通过同态 f）到环 A 中的**限制**，或者叫作是 $\mathfrak{b}$ 在 A 中的**限制理想**，表示成 $\mathfrak{b}^c$. 我们注意，理想的扩张和限制运算不仅与环 A 和 B 有关，而且是依赖于某个环同态 $f:A\to B$ 的. 特别若 A 是 B 的一个子环，而且 $f:A\to B$ 是**包含映射**（即对于每个 $a\in A$，令 $f(a)=a\in B$），则 $\mathfrak{a}^e=\mathfrak{a}B,\mathfrak{b}^c=\mathfrak{b}\cap A$.

上面所介绍的理想之间的各种运算具有一些简单的性质. 这些性质几乎均可由运算的定义直接推出，我们将它们全部作为习题列在下面.

习　题

1. 环 R 中理想的和、交、积运算均满足交换律与结合律，并且有如下的分配律：设 $\mathfrak{a},\mathfrak{b},\mathfrak{c}$ 为 R 的理想，则

$$\mathfrak{a}(\mathfrak{b}+\mathfrak{c})=\mathfrak{ab}+\mathfrak{ac}.$$

2. 设 $\mathfrak{a},\mathfrak{b},\mathfrak{c},\mathfrak{a}_i,\mathfrak{b}_i$ 均为环 R 的理想，则

$$\mathfrak{a}\subseteq(\mathfrak{a}:\mathfrak{b}),(\mathfrak{a}:\mathfrak{b})\mathfrak{b}\subseteq\mathfrak{a}.$$

$$((\mathfrak{a}:\mathfrak{b}):\mathfrak{c})=(\mathfrak{a}:\mathfrak{bc})=((\mathfrak{a}:\mathfrak{c}):\mathfrak{b}).$$

$$(\mathfrak{a}:(\mathfrak{b}+\mathfrak{c}))=(\mathfrak{a}:\mathfrak{b})\cap(\mathfrak{a}:\mathfrak{c}).$$

$$\left(\bigcap_{i\in I}\mathfrak{a}_i:\mathfrak{b}\right)=\bigcap_{i\in I}(\mathfrak{a}_i:\mathfrak{b}),\quad\left(\mathfrak{a}:\sum_{i\in I}\mathfrak{b}_i\right)=\bigcap_{i\in I}(\mathfrak{a}:\mathfrak{b}_i).$$

3. 设 $f:A\to B$ 为环的同态，$\mathfrak{a}$ 和 $\mathfrak{b}$ 分别是环 A 和 B 中的理想，求证：

(1) $\mathfrak{a}\subseteq\mathfrak{a}^{ec}$, $\mathfrak{b}\supseteq\mathfrak{b}^{ce}$, $\mathfrak{b}^{c}=\mathfrak{b}^{cec}$, $\mathfrak{a}^{e}=\mathfrak{a}^{ece}$.

(2) 以 C 表示 A 中全部限制理想，以 E 表示 B 中全部扩张理想，即

$C=\{\mathfrak{b}^{c}\mid \mathfrak{b}$ 为环 B 的理想$\}$，$E=\{\mathfrak{a}^{e}\mid \mathfrak{a}$ 为环 A 的理想$\}$。

则 $f:C\to E$，$\mathfrak{a}\mapsto\mathfrak{a}^{e}$ 和 $g:E\to C$，$\mathfrak{b}\mapsto\mathfrak{b}^{c}$ 是互逆的映射。从而给出集合 C 和集合 E 之间的一一对应。

4．设 $f:A\to B$ 为环的同态，$\mathfrak{a}_1,\mathfrak{a}_2$ 为 A 的理想，$\mathfrak{b}_1,\mathfrak{b}_2$ 为 B 的理想，则

$$(\mathfrak{a}_1+\mathfrak{a}_2)^{e}=\mathfrak{a}_1^{e}+\mathfrak{a}_2^{e},\ (\mathfrak{b}_1+\mathfrak{b}_2)^{c}\supseteq\mathfrak{b}_1^{c}+\mathfrak{b}_2^{c}.$$

$$(\mathfrak{a}_1\cap\mathfrak{a}_2)^{e}\subseteq\mathfrak{a}_1^{e}\cap\mathfrak{a}_2^{e},\ (\mathfrak{b}_1\cap\mathfrak{b}_2)^{c}=\mathfrak{b}_1^{c}\cap\mathfrak{b}_2^{c}.$$

$$(\mathfrak{a}_1\mathfrak{a}_2)^{e}=\mathfrak{a}_1^{e}\mathfrak{a}_2^{e},\ (\mathfrak{b}_1\mathfrak{b}_2)^{c}\supseteq\mathfrak{b}_1^{c}\cdot\mathfrak{b}_2^{c}.$$

$$(\mathfrak{a}_1:\mathfrak{a}_2)^{e}\subseteq(\mathfrak{a}_1^{e}:\mathfrak{a}_2^{e}),\ (\mathfrak{b}_1:\mathfrak{b}_1)^{c}\subseteq(\mathfrak{b}_1^{c}:\mathfrak{b}_2^{c}).$$

并且举例说明以上诸式中的⊆或⊇一般均不能改成等号。

5．设 $\mathbf{Z}$ 为整数环，$m,n\in\mathbf{Z}$，$m,n\geqslant0$，$\mathfrak{a}=n\mathbf{Z}$，$\mathfrak{b}=m\mathbf{Z}$。求证

(1) $\mathfrak{a}+\mathfrak{b}=(m,n)\mathbf{Z}$，$\mathfrak{a}\cap\mathfrak{b}=[m,n]\mathbf{Z}$，$\mathfrak{a}\mathfrak{b}=mn\mathbf{Z}$，其中 (m,n) 和 $[m,n]$ 分别表示 m 和 n 的最大公约数和最小公倍数。

(2) $\mathfrak{a}$ 和 $\mathfrak{b}$ 互素 $\Longleftrightarrow(m,n)=1\Longleftrightarrow\mathfrak{a}\cap\mathfrak{b}=\mathfrak{a}\mathfrak{b}$。

(3) $(\mathfrak{a}:\mathfrak{b})=q\mathbf{Z}$，其中 $q=n/(n,\ m)$

6．一般地，设 $\mathfrak{a}$ 和 $\mathfrak{b}$ 是环 R 的两个理想，则：$\mathfrak{a}$ 与 $\mathfrak{b}$ 互素 $\Longleftrightarrow\mathfrak{a}\cap\mathfrak{b}=\mathfrak{a}\mathfrak{b}$。

7．（中国剩余定理） 设 $\mathfrak{a}_1\cdots,\mathfrak{a}_n$ 是环 R 的 n 个理想，并且它们两两互素。求证有环的同构

$$f:R/\mathfrak{a}_1\cap\cdots\cap\mathfrak{a}_n\cong R/\mathfrak{a}_1\oplus R/\mathfrak{a}_2\oplus\cdots\oplus R/\mathfrak{a}_n,$$

$$x(\mathrm{mod}\ \mathfrak{a}_1\cap\cdots\cap\mathfrak{a}_n)\mapsto(x(\mathrm{mod}\ \mathfrak{a}_1),\ x(\mathrm{mod}\ \mathfrak{a}_2),\cdots,x(\mathrm{mod}\,\mathfrak{a}_n)),$$

其中⊕表示环的直和，而对每个理想 $\mathfrak{a}$ 和 $x\in R$，我们以 $x(\mathrm{mod}\ \mathfrak{a})$ 表示 x 在商环 $R/\mathfrak{a}$ 中的标准同态象。

§1.2 素理想和极大理想

设 R 是非零环，R 中的理想 $\mathfrak{p}$ 叫作是**素理想**，是指它满足以下两个条件：

(i) $\mathfrak{p}\neq R$；

(ii) 如果 $a,b\in R, ab\in\mathfrak{p}$,则 $a\in\mathfrak{p}$ 或者 $b\in\mathfrak{p}$.

而 R 中理想 $\mathfrak{m}$ 叫作是**极大理想**,是指它满足以下两个条件:

(i′) $\mathfrak{m}\neq R$;

(ii′) $\mathfrak{m}$ 和 R 之间不存在 R 的理想. 换句话说,如果 $\mathfrak{a}$ 是 R 中的理想并且 $\mathfrak{m}\subseteq\mathfrak{a}\subseteq R$ 则 $\mathfrak{a}=\mathfrak{m}$ 或者 $\mathfrak{a}=R$.

定理 1 设 $\mathfrak{a}$ 是非零环 R 的理想,则

(1) $\mathfrak{a}$ 为 R 的素理想 $\Longleftrightarrow$ 商环 $R/\mathfrak{a}$ 是整环;

(2) $\mathfrak{a}$ 为 R 的极大理想 $\Longleftrightarrow$ 商环 $R/\mathfrak{a}$ 是域.

证明 (1) 若 $\mathfrak{a}$ 为 R 的素理想,则 $\mathfrak{a}\neq R$,从而 $R/\mathfrak{a}$ 不是零环.进而,设 $\bar{x},\bar{y}\in R/\mathfrak{a}(x,y\in R)$,并且 $\bar{x}\cdot\bar{y}=\bar{0}\in R/\mathfrak{a}$,则 $\overline{xy}=\bar{x}\cdot\bar{y}=\bar{0}$,从而 $xy\in\mathfrak{a}$. 由于 $\mathfrak{a}$ 为素理想,从而 $x\in\mathfrak{a}$ 或者 $y\in\mathfrak{a}$,即 $\bar{x}=\bar{0}$ 或者 $\bar{y}=\bar{0}$. 这就表明 $R/\mathfrak{a}$ 中没有非零的零因子,即 $R/\mathfrak{a}$ 是整环. 反过来,如果 $R/\mathfrak{a}$ 为整环,则 $R/\mathfrak{a}\neq(0)$,即 $\mathfrak{a}\neq R$. 进而,如果 $x,y\in R,xy\in\mathfrak{a}$,则 $\bar{x}\cdot\bar{y}=\overline{xy}=\bar{0}\in R/\mathfrak{a}$,由于$R/\mathfrak{a}$是整环,从而 $\bar{x}=\bar{0}$ 或者 $\bar{y}=\bar{0}$,即 $x\in\mathfrak{a}$ 或者 $y\in\mathfrak{a}$,这就表明 $\mathfrak{a}$ 是 R 的素理想.

(2) 若 $\mathfrak{a}$ 为 R 的极大理想,则 $R/\mathfrak{a}\neq(0)$,并且对于 $R/\mathfrak{a}$ 中每个非零元素 $\bar{x}$(即 $\bar{x}\neq\bar{0},x\in R$),则 $x\notin\mathfrak{a}$. 于是由 x 和 $\mathfrak{a}$ 所生成的理想 $xR+\mathfrak{a}$ 大于 $\mathfrak{a}$. 由 $\mathfrak{a}$ 的极大性即知 $xR+\mathfrak{a}=R$. 由于 $1\in R$,从而存在 $r\in R$ 和 $a\in\mathfrak{a}$,使得 $xr+a=1$. 因此 $\bar{x}\cdot\bar{r}=\overline{xr}=\overline{1-a}=\bar{1}-\bar{a}=\bar{1}-\bar{0}=\bar{1}\in R/\mathfrak{a}$. 这就表明非零商环 $R/\mathfrak{a}$ 中每个非零元素 $\bar{x}$ 均有乘法逆元素. 于是 $R/\mathfrak{a}$ 为域. 反过来,如果$R/\mathfrak{a}$ 为域,则 $R/\mathfrak{a}\neq(0)$,于是 $\mathfrak{a}\neq R$. 进而,假设 $\mathfrak{b}$ 为 R 的理想并且 $\mathfrak{a}\subseteq\mathfrak{b}\subseteq R$. 如果 $\mathfrak{a}\neq\mathfrak{b}$,则有 $x\in\mathfrak{b},x\notin\mathfrak{a}$. 从而在 $R/\mathfrak{a}$ 中 $\bar{x}\neq\bar{0}$. 由于 $R/\mathfrak{a}$ 为域,于是有 $r\in R$,使得 $\bar{x}\bar{r}=\bar{1}$,即 $xr-1\in\mathfrak{a}$. 于是 $1\in xr+\mathfrak{a}\subseteq xR+\mathfrak{a}\subseteq\mathfrak{b}$. 这就表明 $\mathfrak{b}=R$. 从而 $\mathfrak{a}$ 是 R 的极大理想. ▌

注记 1. 我们知道,域中非零元素 x 均有乘法逆元素,从而 x 不为零因子($xr=0\Rightarrow r=x^{-1}xr=0$). 这表明域必是整环. 于是

由定理 1 可知，环 R 的每个极大理想必然是素理想. 但是反过来，素理想不一定是极大理想. 例如，对于多项式环 $R=\mathbf{Z}[x]$，(x) 为素理想，从而 $\mathbf{Z}[x]/(x)\cong\mathbf{Z}$ 是整环，但是 $\mathbf{Z}$ 不为域，从而 (x) 不是 R 的极大理想. 事实上我们有 $(x)\subset(2,x)\subset\mathbf{Z}[x]$，而 $(2,x)$ 为 $\mathbf{Z}[x]$ 的极大理想，因为商环 $\mathbf{Z}[x]/(2,x)\cong\mathbf{Z}/2\mathbf{Z}$ 是二元域.

2. 由定理 1 可知：(0) 为环 R 的素理想 $\Longleftrightarrow R$ 为整环；(0) 为 R 的极大理想 $\Longleftrightarrow R$ 为域.

人们自然会提出一个很基本的问题：每个非零环是否至少存在一个极大理想和素理想？答案是肯定的. 为了证明这一点，我们需要用集合论中一个重要结果，叫作 Zorn 引理. 因为今后我们不断地使用它，所以我们现在介绍什么是 Zorn 引理，关于它的证明和一些等价形式请参看集合论的书.

集合 Σ 上的一个二元关系 $\leqslant$ 叫作是 Σ 上的一个**部分序**，是指关于 $\leqslant$ 满足以下三个条件：对于任意 $x,y,z\in\Sigma$，

(i) $x\leqslant x$；

(ii) 如果 $x\leqslant y$，$y\leqslant x$，则 $x=y$；

(iii) 如果 $x\leqslant y$，$y\leqslant z$，则 $x\leqslant z$.

这时称 $(\Sigma,\leqslant)$ 是一个部分序集合. 所谓"部分"的意思是指，在 Σ 中可能有元素 x,y，使得 $x\leqslant y$ 和 $y\leqslant x$ 均不成立. 如果是这种情形，则称 x 和 y 是**不可比较的**. 否则，即如果 $x\leqslant y$ 或 $y\leqslant x$ 至少有一个成立，则称 x 和 y 是**可比较的**. 设 Σ' 是部分序集合 $(\Sigma,\leqslant)$ 的一个子集合. 如果 Σ' 中任意两个元素均可比较，则称 Σ' 是一个**链**. Σ 中元素 x 叫作是子集合 Σ' 的**上界**，是指对每个 $s\in\Sigma'$ 均有 $s\leqslant x$. Σ' 中元素 x 叫作是 Σ' 的一个**极大元**，是指对于 Σ' 中每个与 x 可比较的元素 y，必然 $y\leqslant x$.

Zorn 引理 设 $(\Sigma,\leqslant)$ 是非空的部分序集合. 如果 Σ 中每个

链在 Σ 中均有上界，则 Σ 必有极大元.

现在我们用 Zorn 引理来证明非零环中极大理想的存在性.我们甚至可以证明更强的结果.

定理 2 设 $\mathfrak{a}$ 是非零环 R 中的真理想(即 $\mathfrak{a}\neq R$)，则 R中存在极大理想 $\mathfrak{m}$,使得 $\mathfrak{m}\supseteq\mathfrak{a}$.

证明 考虑集合

$$\Sigma=\{\mathfrak{b}\mid\mathfrak{b}\text{ 为 }R\text{ 的理想,且 }\mathfrak{a}\subseteq\mathfrak{b}\neq R\}.$$

由于 $\mathfrak{a}\in\Sigma$,从而 Σ 是非空集合. 集合论的包含关系$\subseteq$显然是 Σ 中的部分序,从而$(\Sigma,\subseteq)$是非空部分序集合. 设 Σ'是 Σ 中的一个链. 令 $\mathfrak{c}=\bigcup\limits_{\mathfrak{b}\in\Sigma'}\mathfrak{b}$(集合论的并集). 我们来证明

(i) $\mathfrak{c}$ 是 R 的一个理想,这是因为：如果 $x_1,x_2\in\mathfrak{c}$,由 $\mathfrak{c}$的定义可知有 $\mathfrak{b}_1,\mathfrak{b}_2\in\Sigma'$,使得 $x_1\in\mathfrak{b}_1,x_2\in\mathfrak{b}_2$,由于$\Sigma'$ 为链,于是 $\mathfrak{b}_1\subseteq\mathfrak{b}_2$ 或者 $\mathfrak{b}_2\subseteq\mathfrak{b}_1$. 从而 x_1 和 x_2 或者均属于 $\mathfrak{b}_1$ 或者均属于 $\mathfrak{b}_2$. 因此 $x_1\pm x_2\in\mathfrak{b}_1\cup\mathfrak{b}_2\subseteq\mathfrak{c}$. 同样地,如果 $r\in R,x\in\mathfrak{c}$, 则有 $\mathfrak{b}\in\Sigma'$ 使得 $x\in\mathfrak{b}$. 由于 Σ'中成员 $\mathfrak{b}$ 是理想,从而 $rx\in\mathfrak{b}\subseteq\mathfrak{c}$. 这就表明 $\mathfrak{c}$ 是 R 的理想.

(ii) $\mathfrak{a}\subseteq\mathfrak{c}\neq R$.$\mathfrak{a}\subseteq\mathfrak{c}$ 显然成立.另一方面,如果 $\mathfrak{c}=R$,则 $1\in\mathfrak{c}$,于是有 $\mathfrak{b}\in\Sigma'$ 使得 $1\in\mathfrak{b}$,即 $\mathfrak{b}=R$. 这与 $\mathfrak{b}\in\Sigma'\subseteq\Sigma$ 以及 Σ 的定义相矛盾. 因此 $\mathfrak{c}\neq R$.

综合(i)和(ii)可知 $\mathfrak{c}\in\Sigma$,并且 $\mathfrak{c}$ 显然是链 Σ' 的上界. 于是$(\Sigma,\subseteq)$满足 Zorn 引理条件. 从而 Σ 必有极大元 $\mathfrak{m}$. 于是 $\mathfrak{m}$ 也就是 R 的极大理想并且 $\mathfrak{m}\supseteq\mathfrak{a}$. ▌

注记 1. 由于每个极大理想均是素理想,从而由定理 2 可知,非零环的每个真理想均包含在某个素理想之中.

2. 在定理 2 中取 $\mathfrak{a}=(0)$,即知每个非零环都至少存在一个极大理想,从而也必然存在素理想.

今后我们以 Spec R 表示环 R 的全部素理想组成的集合，把它叫作是环 R 的**素谱**. 而 R 的全部极大理想组成的集合叫作是环 R 的**极大谱**，表示成 Max R. 于是，对于每个非零环 R，我们有 $\varnothing \neq \text{Max } R \subseteq \text{Spec } R$.

定义 只有一个极大理想的非零环叫作是**局部环**. 只有有限个极大理想的非零环叫作是**半局部环**.

如果 R 为局部环，$\mathfrak{m}$ 是它的唯一极大理想，则这个局部环也表成为$(R, \mathfrak{m})$. 域 $R/\mathfrak{m}$ 叫作是局部环的**剩余类域**. 下面定理给出局部环的另一些很有益的刻画方式(注意：环 R 中乘法可逆元叫作是环 R 的**单位**. 环 R 中全部单位形成乘法群，叫作是环 R 的**单位群**，表示成 $U(R)$).

定理 3 设 R 为环而 $\mathfrak{m}$ 是 R 的真理想. 则下列三条件是彼此等价的：

(1) R 为局部环并且 $\mathfrak{m}$ 是它的唯一极大理想；

(2) $R - \mathfrak{m} = U(R)$；

(3) $\mathfrak{m}$ 是 R 的极大理想并且 $1 + \mathfrak{m} \subseteq U(R)$.

证明 (1)⇒(2)：由于 $\mathfrak{m}$ 是真理想，从而 $\mathfrak{m}$ 不能包含单位(注意：$u \in U(R) \Longleftrightarrow (u) = R$). 于是 $R - \mathfrak{m} \supseteq U(R)$. 另一方面，对于每个元素 $u \in R - U(R)$，则(u)为 R 的真理想，从而(u)包含在 R 的某个极大理想之中(定理 2). 但是 R 只有一个极大理想 $\mathfrak{m}$，于是$(u) \subseteq \mathfrak{m}$，特别地 $u \in \mathfrak{m}$. 从而 $R - U(R) \subseteq \mathfrak{m}$. 这相当于 $R - \mathfrak{m} \subseteq U(R)$. 从而 $R - \mathfrak{m} = U(R)$.

(2)⇒(3)：由 $R - \mathfrak{m} = U(R)$ 可知 $1 \notin \mathfrak{m}$，从而 $\mathfrak{m}$ 是真理想. 由于比 $\mathfrak{m}$ 大的理想必然包含单位，即必然是 R，从而 $\mathfrak{m}$ 是 R 的极大理想. 再用反证法证明 $1 + \mathfrak{m} \subseteq U(R)$. 如果存在 $m \in \mathfrak{m}$，使得 $1 + m \notin U(R)$，则由 $R - \mathfrak{m} = U(R)$ 可知 $1 + m \in \mathfrak{m}$. 于是 $1 \in \mathfrak{m}$,

这不可能．从而 $1+\mathfrak{m}\subseteq U(R)$．

(3)⇒(1)：只需证明 R 只有一个极大理想 $\mathfrak{m}$．设 $\mathfrak{m}'$ 是 R 的任意一个极大理想．如果 $\mathfrak{m}'\neq\mathfrak{m}$，由于 $\mathfrak{m}'$ 和 $\mathfrak{m}$ 均是极大理想，并且 $\mathfrak{m}'+\mathfrak{m}\supset\mathfrak{m}$．从而 $\mathfrak{m}'+\mathfrak{m}=R$．于是有 $m\in\mathfrak{m}$，$m'\in\mathfrak{m}'$，使得 $m+m'=1$．于是 $m'=1-m\in 1+\mathfrak{m}\subseteq U(R)$，从而 $\mathfrak{m}'=R$，这就导致矛盾．于是 $\mathfrak{m}=\mathfrak{m}'$，即 $\mathfrak{m}$ 是 R 的唯一极大理想．▌

例 1 整数环 $\mathbf{Z}$ 为主理想整环，每个理想均有形式 $n\mathbf{Z}$ ($n\in\mathbf{Z}$, $n\geqslant 0$)．不难验证：$\mathbf{Z}/n\mathbf{Z}$ 为整环$\Longleftrightarrow n=0$ 或者素数；$\mathbf{Z}/n\mathbf{Z}$ 为域$\Longleftrightarrow n$ 为素数．于是 $\operatorname{Max}\mathbf{Z}=\{p\mathbf{Z}\mid p\text{ 为素数}\}$，而 $\operatorname{Spec}\mathbf{Z}=\operatorname{Max}\mathbf{Z}\cup\{(0)\}$．

例 2 设 m 为正整数，考虑环 $\mathbf{Z}/m\mathbf{Z}$．设 $m=p_1^{a_1}\cdots p_s^{a_s}$ 是 m 的素因子分解式，其中 $p_1,\cdots,p_s$ 是两两不同的素数，而 $a_i\geqslant 1$ ($1\leqslant i\leqslant s$)．由环的同态定理可知 $\mathbf{Z}/m\mathbf{Z}$ 的每个理想均有形式 $n\mathbf{Z}/m\mathbf{Z}$，其中 $n\mid m$．并且 $(\mathbf{Z}/m\mathbf{Z})/(n\mathbf{Z}/m\mathbf{Z})\cong\mathbf{Z}/n\mathbf{Z}$．从而 $n\mathbf{Z}/m\mathbf{Z}$ 为 $\mathbf{Z}/m\mathbf{Z}$ 的素理想$\Longleftrightarrow\mathbf{Z}/n\mathbf{Z}$ 为整环$\Longleftrightarrow n$ 为素数$\Longleftrightarrow\mathbf{Z}/n\mathbf{Z}$ 为域$\Longleftrightarrow n\mathbf{Z}/m\mathbf{Z}$ 为 $\mathbf{Z}/m\mathbf{Z}$ 的极大理想．从而 $\operatorname{Max}(\mathbf{Z}/m\mathbf{Z})=\operatorname{Spec}(\mathbf{Z}/m\mathbf{Z})=\{p_i\mathbf{Z}/m\mathbf{Z}\mid 1\leqslant i\leqslant s\}$．并且 $\mathbf{Z}/m\mathbf{Z}$ 为局部环$\Longleftrightarrow m$ 为某个素数的幂（即 $s=1$）．

例 3 上面例 2 的 $\mathbf{Z}/m\mathbf{Z}$ ($m\geqslant 1$) 为半局部环．更一般地，每个有限环均是半局部环，因为它的子集只有有限多个．从而极大理想也只有有限多个．

进一步的例子请见习题．

习 题

1．设 $\mathfrak{p}$ 是环 R 的理想．求证：$\mathfrak{p}$ 为 R 的素理想$\Longleftrightarrow$对于 R 的任意两个理想 $\mathfrak{a}$ 和 $\mathfrak{b}$，如果 $\mathfrak{a}\mathfrak{b}\subseteq\mathfrak{p}$，则 $\mathfrak{a}\subseteq\mathfrak{p}$ 或者 $\mathfrak{b}\subseteq\mathfrak{p}$

2．设 $\mathfrak{a}$ 是环 R 的理想，而 $\mathfrak{p}_1,\cdots\mathfrak{p}_n$ 是 R 的素理想．如果 $\mathfrak{a}\subseteq\bigcup_{i=1}^{n}\mathfrak{p}_i$，求证存在 $i(1\leqslant i\leqslant n)$ 使得 $\mathfrak{a}\subseteq\mathfrak{p}_i$．

3．设 $\mathfrak{p}$ 是环 R 的素理想，而 $\mathfrak{a}_1,\cdots,\mathfrak{a}_n$ 是 R 的理想．如果 $\mathfrak{p}=\bigcap_{i=1}^{n}\mathfrak{a}_i$，求证有 $i(1\leqslant i\leqslant n)$ 使得 $\mathfrak{p}=\mathfrak{a}_i$．

4．求证（含有幺元素的交换）有限环中每个素理想必是极大理想．

5．求证：主理想环中的非零素理想必是极大理想．

6．设 k 为域．

(1) 试决定多项式环 $k[x]$ 的素谱和极大谱．

(2) 设 $f(x)\in k[x]$，试决定环 $k[x]/(f)$ 的素谱和极大谱．

7．如果 x 是局部环中的幂等元（即 $x^2=x$），求证 $x=0$ 或者 $x=1$．

8．环 B 叫作是**布尔环**，是指 B 中每个元素均是幂等元．求证在布尔环 B 中，

(1) 对于每个元素 $x\in B$ 均有 $2x=0$．

(2) B 中素理想 $\mathfrak{p}$ 均是极大理想，并且 $B/\mathfrak{p}$ 是二元域．

(3) B 的每个有限生成理想均是主理想．［提示：证明 $(a,b)=(a+b+ab)$］

9．设 $f:A\to B$ 为环的同态．$\mathfrak{a}$ 和 $\mathfrak{b}$ 分别为 A 和 B 的理想．$\mathfrak{a}^e=f(\mathfrak{a})B$，$\mathfrak{b}^c=f^{-1}(\mathfrak{b})$．求证：

(1) 若 $\mathfrak{b}\in\mathrm{Spec}\ B$，则 $\mathfrak{b}^c\in\mathrm{Spec}\ A$；

(2) 若 $\mathfrak{a}\in\mathrm{Spec}\ A$，则不一定 $\mathfrak{a}^e\in\mathrm{Spec}\ B$．

如果将 Spec A 和 Spec B 改成 Max A 和 Max B，那么情况如何？

10．设 $R=k[x_1,\cdots,x_n]$ 是域 k 上关于 n 个文字 $x_1,\cdots,x_n(n\geqslant 1)$ 的多项式环．求证 $\mathrm{Spec}\ R=\mathrm{Max}\ R\cup\{(0)\}\Longleftrightarrow n=1$．

11．用 Zorn 引理证明：非零环中必存在极小素理想．（$\mathfrak{p}$ 叫作是环 R 的**极小素理想**，是指 $\mathfrak{p}\in\mathrm{Spec}\ R$，并且若 $\mathfrak{p}'\in\mathrm{Spec}\ R$ 同时 $\mathfrak{p}'\subseteq\mathfrak{p}$，则必然 $\mathfrak{p}'=\mathfrak{p}$．）

12．设 $\mathfrak{a}_1,\cdots,\mathfrak{a}_n$ 是环 R 的 n 个理想，并且 $\mathfrak{a}_1,\cdots,\mathfrak{a}_n$ 两两互素，求证 $\prod_{i=1}^{n}\mathfrak{a}_i=\bigcap_{i=1}^{n}\mathfrak{a}_i$．

§ 1.3 大根和小根

设 $\mathfrak{a}$ 是环 R 的理想. 定义集合

$$\sqrt{\mathfrak{a}}=\{x\in R \mid \text{存在正整数 } n, \text{ 使得 } x^n\in\mathfrak{a}\}.$$

定理 4 (1) $\sqrt{\mathfrak{a}}$ 是环 R 的理想.

(2) 当 $\mathfrak{a}\neq R$ 时, $\sqrt{\mathfrak{a}}$ 是 R 中包含 $\mathfrak{a}$ 的所有素理想的交,即

$$\sqrt{\mathfrak{a}}=\bigcap_{\substack{\mathfrak{p}\in \operatorname{Spec} R\\ \mathfrak{p}\supseteq\mathfrak{a}}}\mathfrak{p} \qquad (*)$$

证明 我们只需要证明(*)式. 因为显然 $\sqrt{R}=R$, 并且当 $\mathfrak{a}\neq R$ 时, 由(*)式知 $\sqrt{\mathfrak{a}}$ 是一些素理想之交, 从而 $\sqrt{\mathfrak{a}}$ 为理想.

将(*)式右边记为 $\mathfrak{n}$. 先证 $\sqrt{\mathfrak{a}}\subseteq\mathfrak{n}$. 如果 $f\in\sqrt{\mathfrak{a}}$, 则由定义知存在整数 $n\geqslant 1$ 使得 $f^n\in\mathfrak{a}$. 从而对每个素理想 $\mathfrak{p}\supseteq\mathfrak{a}$,均有 $f^n\in\mathfrak{p}$. 于是 $f\in\mathfrak{p}$. 从而 $f\in\mathfrak{n}$. 这就证明了 $\sqrt{\mathfrak{a}}\subseteq\mathfrak{n}$.

再证 $\sqrt{\mathfrak{a}}\supseteq\mathfrak{n}$. 假如 $f\notin\sqrt{\mathfrak{a}}$ 我们只要证明 $f\notin\mathfrak{n}$ 即可. 为此考虑集合

$$\Sigma=\{R \text{ 的理想 } \mathfrak{c} \mid \mathfrak{c}\supseteq\mathfrak{a}, \text{并且对每个正整数 } n \text{ 均有 } f^n\notin\mathfrak{c}\}.$$

由 $f\notin\sqrt{\mathfrak{a}}$ 可知 $\mathfrak{a}\in\Sigma$. 从而 Σ 是非空集合. 设 Σ' 是部分序集 $(\Sigma,\subseteq)$ 的一个链. 可以象定理 2 证明中一样推得 $\mathfrak{c}=\bigcup\limits_{\mathfrak{c}'\in\Sigma'}\mathfrak{c}'$ 是 R 的理想. 并且 $\mathfrak{c}\in\Sigma$ (因为显然有 $\mathfrak{c}\supseteq\mathfrak{a}$. 并且若 $f^n\in\mathfrak{c}$, 则有 $\mathfrak{c}'\in\Sigma'$ 使得 $f^n\in\mathfrak{c}'$,而这与 $\mathfrak{c}'\in\Sigma$ 相矛盾). 于是 $\mathfrak{c}$ 为 Σ' 的上界. 利用 Zorn 引理可知集合 Σ 有极大元 $\mathfrak{p}$. 我们来证 $\mathfrak{p}$ 是 R 的素理想. 假设 $x,y\notin\mathfrak{p}$,则理想 $xR+\mathfrak{p}$ 和 $yR+\mathfrak{p}$ 均大于 $\mathfrak{p}$. 由于 $\mathfrak{p}$ 是 Σ 中极大元,因此 $xR+\mathfrak{p}$ 和 $yR+\mathfrak{p}$ 均不属于 Σ. 于是有 $m,n\geqslant 1$,使得 $f^m\in xR+\mathfrak{p}$, $f^n\in yR+\mathfrak{p}$. 从而 $f^{m+n}\in(xR+\mathfrak{p})(yR+\mathfrak{p})=xyR+\mathfrak{p}$. 这就表明 $xy\notin\mathfrak{p}$ (否则若 $xy\in\mathfrak{p}$ 便有 $f^{m+n}\in\mathfrak{p}$,而这与 $\mathfrak{p}\in\Sigma$ 相矛盾). 于是 $\mathfrak{p}$ 为素理想.

由于 $\mathfrak{p}\in\Sigma$，从而 $f\notin\mathfrak{p}$，注意 $\mathfrak{p}\supseteq\mathfrak{a}$，从而便有 $f\notin\mathfrak{n}$. 这就证明了 $\sqrt{\mathfrak{a}}\supseteq\mathfrak{n}$. 于是 $\sqrt{\mathfrak{a}}=\mathfrak{n}$. ▌

定义 称 $\sqrt{\mathfrak{a}}$ 为理想 $\mathfrak{a}$ 的**根**. 特别地

$$\sqrt{(0)}=\{x\in R\mid \text{存在整数 } n\geqslant 1, \text{使得} x^n=0\}$$

$$=R \text{ 中幂零元全体}=\bigcap_{\mathfrak{p}\in \operatorname{Spec} R}\mathfrak{p} \quad (\text{定理 } 4).$$

我们把 $\sqrt{(0)}$ 叫作是环 R 的**幂零根**(因为它是 R 中幂零元素全体所组成的理想)，并且记为 $N(R)$. 由定理 4，它也是 R 中全体素理想之交. 与此类似，我们还有环 R 中另一个理想

$$r(R)=\bigcap_{\mathfrak{m}\in \operatorname{Max} R}\mathfrak{m}.$$

即 $r(R)$ 是环 R 中全体极大理想之交，叫作是环 R 的 **Jacobson 根**. 由于 $\operatorname{Spec} R\supseteq\operatorname{Max} R$，可知 $N(R)\subseteq r(R)$. 所以我们今后更形象地把 $N(R)$ 和 $r(R)$ 分别叫作是环 R 的**小根**和**大根**. 下面给出大根的另一种刻画方式.

定理 5 $r(R)=\{x\in R\mid 1-xR\subseteq U(R)\}$.

证明 将上式右边记为 $\mathfrak{a}$. 如果 $x\notin\mathfrak{a}$，则存在 $y\in R$，使得 $1-xy\notin U(R)$，于是 $1-xy$ 包含在 R 的某个极大理想 $\mathfrak{m}$ 之中. 如果 $x\in r(R)$，则 $x\in\mathfrak{m}$. 从而 $1=xy+(1-xy)\in\mathfrak{m}$. 这是不可能的. 因此对每个 $x\notin\mathfrak{a}$ 均有 $x\notin r(R)$. 这表明 $\mathfrak{a}\supseteq r(R)$.

反之，如果 $x\notin r(R)$，则有极大理想 $\mathfrak{m}$ 使得 $x\notin\mathfrak{m}$. 于是 $xR+\mathfrak{m}=R$. 从而有 $m\in\mathfrak{m}, y\in R$ 使得 $xy+m=1$. 于是 $1-xy\in\mathfrak{m}$. 所以 $1-xy\notin U(R)$. 这就表明 $x\notin\mathfrak{a}$. 因此又有 $\mathfrak{a}\subseteq r(R)$. ▌

定理 6 设 $\mathfrak{a},\mathfrak{a}_i$ 均是环 R 的理想. 则

(1) $\sqrt{\bigcap_{i=1}^{n}\mathfrak{a}_i}=\bigcap_{i=1}^{n}\sqrt{\mathfrak{a}_i}$，$\sqrt{\bigcup_{i\in I}\mathfrak{a}_i}=\bigcup_{i\in I}\sqrt{\mathfrak{a}_i}$.

(2) $\sqrt{\mathfrak{a}}=R \Longleftrightarrow \mathfrak{a}=R$.

(3) $\sqrt{\sqrt{\mathfrak{a}}}=\sqrt{\mathfrak{a}}$.

(4) 若 $\mathfrak{p}\in \operatorname{Spec} R$,则对每个整数 $n\geqslant 1$ 均有$\sqrt{\mathfrak{p}^n}=\mathfrak{p}$.

证明 (1) 读者自证.

(2) 利用 $1\in R$ 即可.

(3) 显然$\sqrt{\sqrt{\mathfrak{a}}}\supseteq\sqrt{\mathfrak{a}}$. 反之若 $x\in\sqrt{\sqrt{\mathfrak{a}}}$,则有 $n\geqslant 1$ 使得 $x^n\in\sqrt{\mathfrak{a}}$,于是又有 $m\geqslant 1$,使得$(x^n)^m\in\mathfrak{a}$. 即 $x^{nm}\in\mathfrak{a}$. 从而 $x\in\sqrt{\mathfrak{a}}$, 即$\sqrt{\sqrt{\mathfrak{a}}}\subseteq\sqrt{\mathfrak{a}}$.

(4) 显然有 $\mathfrak{p}\subseteq\sqrt{\mathfrak{p}^n}$(因为 $x\in\mathfrak{p}\Rightarrow x^n\in\mathfrak{p}^n$). 反之,若 $x\in\sqrt{\mathfrak{p}^n}$,则有$m\geqslant 1$,使得 $x^m\in\mathfrak{p}^n\subseteq\mathfrak{p}$,即$x^m\in\mathfrak{p}$. 由于 $\mathfrak{p}$ 为素理想,从而 $x\in\mathfrak{p}$, 即 $\mathfrak{p}\supseteq\sqrt{\mathfrak{p}^n}$. ▌

例 考虑整数环 $\mathbf{Z}$ 和它的理想$m\mathbf{Z}$. 对于 $m=0$,由于 $\mathbf{Z}$ 是整环,即幂零元素只有 0. 从而 $\mathbf{Z}$的小根为(0). 如果$m=1$,$\sqrt{(1)}=\sqrt{\mathbf{Z}}=\mathbf{Z}$. 最后,如果 $m\geqslant 2$,设 $m=p_1^{\alpha_1}\cdots p_s^{\alpha_s}$,$p_1\cdots,p_s$ 为s个不同的素数,$s\geqslant 1,\alpha_i\geqslant 1(1\leqslant i\leqslant s)$. 则由定理 6 可知

$$\begin{aligned}\sqrt{m\mathbf{Z}}&=\sqrt{(p_1^{\alpha_1})\cap\cdots\cap(p_s^{\alpha_s})}=\sqrt{(p_1^{\alpha_1})}\cap\cdots\cap\sqrt{(p_s^{\alpha_s})}\\&=\sqrt{(p_1)^{\alpha_1}}\cap\cdots\cap\sqrt{(p_s)^{\alpha_s}}\\&=(p_1)\cap\cdots\cap(p_s)=(p_1\cdots p_s).\end{aligned}$$

关于$\sqrt{\mathfrak{a}}$的另一些性质请见习题.

习　题

1. 设 $\mathfrak{a}$ 和 $\mathfrak{b}$ 为 R 的两个理想, 则

(1) $\sqrt{\mathfrak{a}+\mathfrak{b}}=\sqrt{\sqrt{\mathfrak{a}}+\sqrt{\mathfrak{b}}}$.

(2) $\sqrt{\mathfrak{a}}$和$\sqrt{\mathfrak{b}}$互素$\Longleftrightarrow\mathfrak{a}$和$\mathfrak{b}$互素.

2．设$\mathfrak{a}$是环R的真理想，则：$\mathfrak{a}=\sqrt{\mathfrak{a}}\Longleftrightarrow\mathfrak{a}$是一些素理想的交.

3．整数环$\mathbf{Z}$和多项式环$k[x_1,\cdots x_n]$(k为域)的大根是什么?

4．求证$N(R/N(R))=(0)$.

5．以D表示环R中全体零因子组成的集合，求证：

$$D=\bigcup_{\substack{x\in R\\x\neq 0}}\sqrt{\mathrm{Ann}(x)}.$$

6．设$f:A\to B$为环的同态．$\mathfrak{a}$和$\mathfrak{b}$分别是A和B的理想．求证：

(1) $(\sqrt{\mathfrak{a}})^e\subseteq\sqrt{\mathfrak{a}^e}$,而等式不一定成立.

(2) $(\sqrt{\mathfrak{b}})^c=\sqrt{\mathfrak{b}^c}$.

7．求证关于环R的以下三条件彼此等价：

(1) R只有一个素理想；

(2) $R-N(R)=U(R)$；

(3) $R/N(R)$为域.

8．设R为环．如果$x\in N(R),y\in U(R)$,求证$x+y\in U(R)$.

9．设R为环．$f(x)=a_0+a_1x+\cdots+a_nx^n\in R[x]$．求证：

(1) $f\in U(R[x])\Longleftrightarrow a_0\in U(R)$并且$a_1,\cdots,a_n\in N(R)$.

(2) $f\in N(R[x])\Longleftrightarrow a_0,a_1,\cdots,a_n\in N(R)$.

(3) f是$R[x]$中的零因子$\Longleftrightarrow$存在$a\in R,a\neq0$,使得$af=0$.

(4) 环$R[x]$的小根等于大根，并且均等于$N(R)[x]$.

10．设R为环,而$R[[x]]$是R上的形式幂级数环．$f(x)=\sum_{n=0}^{\infty}a_nx^n\in R[[x]]$．求证：

(1) $f\in U(R[[x]])\Longleftrightarrow a_0\in U(R)$.

(2) $N(R[[x]])\subseteq N(R)[[x]]$．试问等号是否一定成立?

(3) f属于$R[[x]]$的大根$\Longleftrightarrow a_0$属于R的大根.

(4) 设$\mathfrak{m}\in\mathrm{Max}R[[x]],\mathfrak{m}^c=\mathfrak{m}\cap R$,则$\mathfrak{m}^c\in\mathrm{Max}\,R$,并且$\mathfrak{m}=(\mathfrak{m}^c,x)$.

(5) R中每个素理想均是$R[[x]]$中某个素理想的限制.

11．如果在环R中对于每个元素x均存在$n>1$(n可能依赖于x)使得$x^n=x$．求证$\mathrm{Max}R=\mathrm{Spec}R$.

第二章　模 论 初 步

模论是现代数学中愈来愈重要的工具．它统一了许多数学结构．我们在本章中要介绍模论的初步知识，在以后各章中将要用它作为研究交换代数的基本工具．

§ 2.1　模和它的基本性质

定义　设R是(具有幺元素的交换)环．集合M叫作是环R上的一个**模**或简记为**R-模**，是指M是加法Abel群，并且定义了R中元素与M中元素的一个乘法，即定义了一个映射

$$R\times M\to M,(r,x)\mapsto rx\in M\quad(r\in R,x\in M),$$

使得满足以下诸条件：对于每个$r,s\in R,x,y\in M$，

(1) $r(x+y)=rx+ry$；

(2) $(r+s)x=rx+sx$；

(3) $(rs)x=r(sx)$；

(4) $1_Rx=x$．(1_R表示环R的幺元素)

其中R称为这个模的**系数环**．

注记　由以上定义不难推出：

$$r0_M=0_M,0_Rx=0_M,(-r)x=-(rx)=r(-x),$$

$$n(rx)=(nr)x=r(nx)\quad(\text{对每个 }n\in\mathbf{Z}).$$

为符号简单起见，今后我们将M中零元素0_M，R中零元素0_R以及数零均写成0而不致于引起混乱．

以下诸例表明模这个概念统一了许多代数结构．

例 1　只有一个元素0的R-模叫作是**零模**，表示成(0)．

例 2　设A为任意加法Abel群．象通常那样，对于每个自然数n和$a\in A$，令$na=a+a+\cdots+a$(n个)，而$(-n)a=-na$，

$0a=0$. 不难验证，对于这种运算 A 成为 $\mathbf{Z}$-模. 换句话说，每个 Abel 群均由此种方式自然地看成是 $\mathbf{Z}$-模. 从而由模论应当给出 Abel 群的一些结果(见 §2.7).

例 3 如果 R 是域，则上述的 R-模定义与通常线性代数中"域 R 上向量空间"的定义是一致的，因此模论应当给出线性代数的一些结果(见 §2.2 和 §2.7).

例 4 环 R 本身可看作是 R-模，其中模的乘法就是环 R 中的乘法. 更一般地，对于环 R 的每个子环 A，R 均可看成是 A-模. 例如 $R[x]$ 可看成是 R-模，有理数域 $\mathbf{Q}$ 可看成是 $\mathbf{Z}$-模等等. 另一方面，环 R 的每个理想 $\mathfrak{a}$ 也是 R-模. 例如 $n\mathbf{Z}$ 是 $\mathbf{Z}$-模. 这一切预示着由模论可以研究环的性质.

例 5 (系数环的改变) 设 $f: A\rightarrow B$ 是环的同态. 如果 M 为 B-模. 对于 $a\in A$ 和 $x\in M$，定义 $ax=f(a)x$. 请读者验证，M 由此而成为 A-模.. 这是改变系数环的常用手法.

例 6 设 R 为环而 M 为 R-模. 如果 $\mathfrak{a}$ 是 R 的理想并且 $\mathfrak{a}M=(0)$，其中 $\mathfrak{a}M=\{ax\,|\,a\in\mathfrak{a}, x\in M\}$. 这时我们对于 $\bar{r}\in R/\mathfrak{a}$ $(r\in R)$ 和 $x\in M$ 定义运算 $\bar{r}m=rm$. 易知这个运算是可定义的，也就是说，由 $\mathfrak{a}M=(0)$ 不难推出这个定义与 $\bar{r}$ 中代表元 r 的选取无关 $(\bar{r}=\bar{s}\Rightarrow r-s\in\mathfrak{a}\Rightarrow(r-s)x=0\Rightarrow\bar{r}x=rx=sx=\bar{s}x)$. 并且由此使 M 成为 $R/\mathfrak{a}$-模.

令 $\mathrm{Ann}(M)=\{a\in R\,|\,aM=(0)\}$. 这是环 R 的理想，叫作是**模 M 的零化理想**. 显然 $\mathrm{Ann}(M)M=(0)$. 如果 $\mathrm{Ann}(M)=(0)$ (即是 R 的零理想)，则称 M 是**忠实 R-模**. 换句话说，M 是忠实 R-模指的是：R 中元素 a 如果使 $aM=(0)$，则必然 $a=0$. 由于 $\mathrm{Ann}(M)M=(0)$，从而由例 6 可知 M 可看成是 $R/\mathrm{Ann}(M)$-模. 不难证明 M 是忠实的 $R/\mathrm{Ann}(M)$-模(习题 4).

象群论那样，我们也有子模、商模、模的同态和同构等概念以

及模的同态基本定理.

定义 设 R 为环而 M 为 R-模. M 的子集合 N 如果对于 M 中的运算形成 R-模,则称 N 是 M 的 **R-子模**. 换句话说,N 是 M 的 R-子模当且仅当 N 是 M 的子集合,并且:

(1) $x,y\in N\Rightarrow x\pm y\in N$(即 N 是 M 的 Abel 子群);

(2) $r\in R,x\in N\Rightarrow rx\in N$(即 N 对于 R-作用是封闭的).

例 对于 Abel 群 A,A 的 $\mathbf{Z}$-子模即是 A 的子群(这时条件(2)自然成立.)如果 R 是域,则 R-模 M 的 R-子模恰好就是 R-向量空间 M 的子空间. 如果将 R 看作是 R-模,则由定义不难看出,R 的 R-子模恰好就是 R 的理想.

设 M 是 R-模而 N 是 M 的 R-子模. 根据定义,N 是 Abel 群 M 的子群,从而我们有加法商群 M/N. M/N 中的元素均有形式 $x+N(x\in M)$,表示成 $\bar{x}$. 而加法为 $\bar{x}+\bar{y}=\overline{x+y}$. 现在对于 $r\in R$ 我们定义 $r\bar{x}=\overline{rx}$. 由于 N 是 R-模,可知此定义与 $\bar{x}$ 中代表元的选取无关 ($\bar{x}=\bar{y}\Rightarrow x-y\in N\Rightarrow rx-ry=r(x-y)\in RN\subseteq N\Rightarrow\overline{rx}=\overline{ry}$). 并且可直接验证 M/N 由此而成为 R-模,叫作是 M 对于子模 N 的 **R-商模**.

定义 设 M 和 N 均为 R-模. 映射 $f:M\rightarrow N$ 叫作是 **R-模同态**,是指对任意 $x,y\in M$ 和 $r\in R$,均有

(1) $f(x+y)=f(x)+f(y)$(即 f 为加法群的同态),

(2) $f(rx)=rf(x)$(即 f 与 R-作用可交换).

如果 f 又是单射,满射或者一一对应,则它分别称作是 **R-模单同态,满同态或者同构**.

从 R-模 M 到 R-模 N 的全部 R-模同态所成的集合表示成 $\mathrm{Hom}_R(M,N)$. 对于 $f,g\in\mathrm{Hom}_R(M,N)$,我们定义

$$f+g:M\rightarrow N,(f+g)(x)=f(x)+g(x)(x\in M)$$

直接可以验证，如此定义的 $f+g$ 仍旧是 R-模同态. 并且由此使$\mathrm{Hom}_R(M,N)$成为 Abel 群，其零元素即是零同态(即将 M 中所有元素均映成 0_N 的同态). 进而，对于 $r\in R$ 和 $f\in\mathrm{Hom}_R(M,N)$，我们定义

$$rf: M\to N, (rf)(x)=rf(x)(x\in M).$$

也可直接验证 $rf\in\mathrm{Hom}_R(M,N)$. 并且由此使 $\mathbf{Hom}_R(M,N)$ **成为 R-模.**

例 对于 Abel 群 G 和 H，$\mathbf{Z}$-模同态 $f:G\to H$ 和 Abel 群同态是一回事. 从而今后把 $\mathrm{Hom}_\mathbf{Z}(G,H)$ 简记成 $\mathrm{Hom}(G,H)$. 另一方面，如果 R 是域，则 R-模同态 $f:M\to N$ 就是线性代数中定义的域 R 上向量空间 M 到向量空间 N 的 R-线性变换.

定理 1(同态基本定理 1) 设 $f:M\to N$ 是 R-模同态. 令

$$\mathrm{Ker}f=\{x\in M\mid f(x)=0\}=f^{-1}(0),$$

$$\mathrm{Im}f=\{f(x)\mid x\in M\}=f(M),$$

分别称作是同态 f 的**核**和**象**. 则

(1) $\mathrm{Ker}f$ 是 M 的 R-子模，$\mathrm{Im}f$ 是 N 的 R-子模.

(2) 我们有 R-模同构

$$\bar{f}: M/\mathrm{Ker}f\cong\mathrm{Im}f, \bar{f}(\bar{x})=f(x)(x\in M).$$

特别若 $f:M\to N$ 是 R-模满同态，则有 R-模同构 $M/\mathrm{Ker}f\overset{\bar{f}}{\cong}N$.

证明 (1) 由群论知道 $\mathrm{Ker}f$ 和 $\mathrm{Im}f$ 均是 Abel 群. 为证它们都是 R-模，只需再证：若 $r\in R, x\in\mathrm{Ker}f, y\in\mathrm{Im}f$，则 $rx\in\mathrm{Ker}f$，$ry\in\mathrm{Im}f$. 而这是很容易的.

(2) 由群论的同态基本定理知道，$\bar{f}$: $M/\mathrm{Ker}f\to\mathrm{Im}f$ 是 Abel 群同构. 为证它是 R-模同构，只需再证 $\bar{f}(r\bar{x})=r\bar{f}(\bar{x})$ $(r\in R, x\in M)$即可. 而这是很容易的，因为 $\bar{f}(r\bar{x})=\bar{f}(\overline{rx})=$ $=f(rx)=rf(x)=r\bar{f}(\bar{x})$. ▌

定理 2(同态基本定理2) 设 M 为 R-模而 N 是 M 的 R-子模. 定义如下两个集合:

$A=\{M$ 的 R-子模 $P \mid P\supseteq N\}$, $B=M/N$ 的 R-子模全体. 则映射 $g:A\rightarrow B, g(P)=P/N$ 是集合 A 与 B 之间的保序一一对应, 并且对每个 $P\in A$, 我们有 R-模同构 $(M/N)/(P/N)\cong M/P$.

证明 令 $\tilde{A}=\{M$ 的加法子群 $\tilde{P} \mid \tilde{P}\supseteq N\}$, $\tilde{B}=M/N$ 的加法子群全体. 我们从群论知道, $\tilde{g}:A\rightarrow B$, $\tilde{g}(\tilde{P})=\tilde{P}/N$ 是集合 $\tilde{A}$ 与 $\tilde{B}$ 之间的保序一一对应. 不难验证, $\tilde{P}$ 为 R-模$\Longleftrightarrow\tilde{P}/N$ 为 R-模. 从而映射 $\tilde{g}$ 在集合 A 上的限制即是映射 g, 并且 $\tilde{g}(\tilde{A})==g(A)=B$. 这就证明了 $g:A\rightarrow B$ 是一一对应. 进而, 由群论知道, $\varphi: M/N\rightarrow M/P, x+N\mapsto x+P(x\in M)$ 是加法群的满同态, 并且 $\mathrm{Ker}\varphi=P/N$. 容易验证事实上 φ 是 R-模满同态. 从而由定理 1 即知我们有 R-模同构 $(M/N)/(P/N)\cong M/P$. ▌

现在我们定义 R-模 M 的子模之间的某些运算. 设 N 和 P 均是 M 的 R-子模. 易知

$$N+P=\{x+y \mid x\in N, y\in P\}$$

也是 M 的 R-子模, 叫作是 N 和 P 的**和**. 类似可定义任意有限个子模的和 $\sum_{i=1}^{n}N_i=N_1+N_2+\cdots+N_n$. 并且这种运算满足交换律和结合律. 另一方面, $N\cap P$ 也是 M 的子模, 称作是 N 和 P 的**交**. 类似地, 可以定义任意多个 R-子模的交, 并且交运算也满足结合律与交换律. 此外, $N+P$ 是包含 N 与 P 的最小子模, 而 $N\cap P$ 是同时包含在 N 与 P 之中的最大子模.

更一般地, 设 X 是 R-模 M 的一个子集合. 考虑集合

$$\{\text{有限和}\sum_i r_ix_i \mid r_i\in R, x_i\in X\}.$$

不难验证这是 M 的 R-子模，并且是包含X的最小子模，我们将它记作$\langle X\rangle$，并且叫作是**由集合X生成的子模**．由一个元素 $x\in M$ 生成的 R-子模显然是$\langle x\rangle=Rx$．如果 X 是有限集合，$X=\{x_1,x_2,\cdots,x_n\}$，则$\langle X\rangle=Rx_1+Rx_2+\cdots+Rx_n=\langle x_1,\cdots,x_n\rangle$．如果$M$本身是可以由有限多个元素生成的 R-模，则称 M 为**有限生成 R-模**．由一个元素生成的 R-模 $M=Rx$ 叫作是**循环 R-模**．

注记 一个模是否有限生成是与其系数环R有关系的．例如有理数域 $\mathbf{Q}$ 看作是 $\mathbf{Q}$-模则为循环模：$\mathbf{Q}=\mathbf{Q}\cdot 1$．但是看作 $\mathbf{Z}$-模(即看作加法 Abel 群)时，$\mathbf{Q}$ 甚至不是有限生成的．(对于任意有限个 $x_1,\cdots,x_n\in\mathbf{Q}$，令 p 为素数，大于 $x_1,x_2,\cdots,x_n$ 的公分母，则$\frac{1}{p}\notin \mathbf{Z}x_1+\cdots+\mathbf{Z}x_n$．)

设 $M_i(i\in I)$是一族 R-模．定义集合

$$\prod_{i\in I}M_i=\{(x_i)_{i\in I}\mid x_i\in M_i\},$$

$$\bigoplus_{i\in I}M_i=\{(x_i)_{i\in I}\mid x_i\in M_i,\text{且只有有限个 } x_i \text{ 不为 } 0\}.$$

我们规定：$(x_i)=(y_i)\Longleftrightarrow$对每个 $i\in I$ 均有 $x_i=y_i$．然后定义运算：

$$(x_i)\pm(y_i)=(x_i+y_i),r(x_i)=(rx_i)(x_i,y_i\in M_i,r\in R).$$

可以直接验证，$\prod\limits_{i\in I}M_i$ 和 $\bigoplus\limits_{i\in I}M_i$ 由此均为 R-模，分别叫作是 R-模 $M_i(i\in I)$的**直积**和**直和**．注意$\bigoplus\limits_{i\in I}M_i$ 是 $\prod\limits_{i\in I}M_i$ 的 R-子模．并且当 I 是有限集合时，直和与直积是一致的．

定理 3 设 M 为 R-模，N 和 P 为 M 的 R-子模，则有 R-模同构$\dfrac{N+P}{N}\cong\dfrac{P}{N\cap P}$．

证明 作映射$P\to(N+P)/N$，$x\mapsto x+N$，证明这是R-模满

同态，并且核为 $P\cap N$. 然后由定理 1 即得到结果. ∎

设 N 和 P 均是 R-模 M 的 R-子模. 定义

$$(N:P)=\{a\in R\mid aP\subseteq N\}.$$

这是 R 的理想. 而 $\mathrm{Ann}(P)=(0:P)=\{a\in R\mid aP=(0)\}$ 叫作是**子模 P 的零化理想**. 于是，M 为忠实 R-模 $\Longleftrightarrow(0:M)=(0)$. 对于 M 中每个元素 x，$\mathrm{Ann}(x)=(0:x)=(0:Rx)=\{a\in R\mid ax=0\}$ 叫作是**元素 x 的零化理想**. 如果 $\mathrm{Ann}(x)\neq(0)$，即存在非零元素 $a\in R$，使得 $ax=0$，则称 x 为 R-模 M 的**扭元素**. 以 $T(M)$ 表示 R-模 M 的全部扭元素组成的集合. 如果 $T(M)=(0)$，我们称 M 是**无扭 R-模**.

引理 1 如果 R 是整环，M 为 R-模，则 $T(M)$ 是 M 的 R-子模，并且 $M/T(M)$ 是无扭 R-模.

证明 设 $x,y\in T(M)$，则有 $r,s\in R-\{0\}$，使得 $rx=sy=0$. 由于 R 是整环，从而 $rs\neq0$，并且 $rs(x\pm y)=s(rx)\pm r(sy)=0$. 从而 $x\pm y\in T(M)$. 类似地，若 $x\in T(M)$，则有 $s\in R-\{0\}$，使得 $sx=0$. 于是对每个 $r\in R$ 均有 $s(rx)=(sr)x=(rs)x=r(sx)=$ $=r\cdot0=0$. 即 $rx\in T(M)$. 这就表明 $T(M)$ 是 M 的 R-子模.

设 $\bar{x}\in T(M/T(M))$，$x\in M$. 则有 $0\neq r\in R$，使得 $r\bar{x}=\bar{0}$，即 $rx\in T(M)$. 于是又有 $0\neq s\in R$，使得 $s(rx)=0$，即 $(sr)x=0$. 由 R 为整环可知 $sr\neq0$. 从而 $x\in T(M)$，即 $\bar{x}=\bar{0}$. 于是 R-模 $M/T(M)$ 只有 $\bar{0}$ 为扭元素，即为无扭 R-模. ∎

注记 如果 R 不是整环，则 $T(M)$ 不一定为 M 的 R-子模. 例如取 $M=\mathbf{Z}/6\mathbf{Z}$ 看作是 $\mathbf{Z}/6\mathbf{Z}$-模，则 $\bar{2},\bar{3}\in T(M)$，但是 $\bar{5}=\bar{2}+\bar{3}\notin T(M)$.

定义 若 R 为整环而 M 为 R-模，我们把子模 $T(M)$ 叫作 M 的**扭子模**.

习　题

1．记 $Z_m = Z/mZ$（m 为正整数）．

（1）求证 $\mathrm{Hom}(Z_m, Z_n) \cong Z_{(m,n)}$（$Z$-模同构）．

（2）求证 $\mathrm{Hom}(Z_m, Z) = (0)$．

（3）对于 Abel 群 A，记 $A[m] = \{a \in A \mid ma = 0\}$．求证 $A[m]$ 是 A 的子群，并且有 Abel 群同构 $\mathrm{Hom}(Z_m, A) \cong A[m]$．

2．试决定 $\mathrm{Hom}(Q, Q)$ 和 $\mathrm{Hom}_Q(Q, Q)$．

3．设 M 为 R-模，求证有 R-模同构 $M \cong \mathrm{Hom}_R(R, M)$．

4．设 M 为 R-模，则 M 为忠实 $R/\mathrm{Ann}(M)$-模．

5．设 N，P，N_1，N_2 均为 R-模 M 的 R-子模，求证：

（1）$\mathrm{Ann}(N_1 + N_2) = \mathrm{Ann}(N_1) \cap \mathrm{Ann}(N_2)$，

（2）$(N : P) = \mathrm{Ann}\left(\dfrac{N+P}{N}\right)$．

6．设 M 为循环 R-模，则有 R 的理想 $\mathfrak{a}$，使得 $M \cong R/\mathfrak{a}$（R-模同构）．

7．R-模 M 叫作是**单模**，是指 M 只有两个平凡的 R-子模：(0) 和 M．求证：

（1）每个单 R-模均是循环模．

（2）如果 M 是单 R-模，则对于任意 R-模 N，R-模同态 $f: M \to N$ 或者为零同态或者为单同态．而 R-模同态 $g: N \to M$ 或者为零同态或者为满同态．最后，R-模自同态 $h: M \to M$ 或者为零同态或者为同构．

（3）M 为单 R-模并且 $M \neq (0) \Longleftrightarrow M \cong R/\mathfrak{m}$（$R$-模同构），其中 $\mathfrak{m}$ 是 R 中某个极大理想．

8．如果 $f \in \mathrm{Hom}_R(M, M)$（$M$ 为 R-模），并且 $f^2 = f$，求证 $M = \mathrm{Ker}\, f \oplus \mathrm{Im}\, f$．

9．设 $f: A \to B$，$g: B \to A$ 均是 R-模同态，并且 $gf = 1_A$（1_A 表示 A 上的恒等自同构），求证 $B = \mathrm{Im}\, f \oplus \mathrm{Ker}\, g$．

10．设 A 是环 B 的子环．如果 M 是有限生成 B-模而 B 是有限生成 A-模，求证 M 是有限生成 A-模．

11．求证域 R 上的模必为无扭模．

§ 2.2 模上的线性代数

我们已经看到，向量空间是模的特殊情形．或者说，模是向量空间的一种推广，即把系数域推广成环．向量空间上线性代数的许多概念也可不同程度地推广到一般模上去．例如线性无关和基这两个概念就是如此．

定义 R-模M的一个子集合S叫作是 **R-线性无关**的，是指：如果 $x_1,\cdots,x_n\in S, r_1,\cdots,r_n\in R, n\geqslant 1$，使得 $r_1x_1+\cdots+r_nx_n=0$，则 $r_1=r_2=\cdots=r_n=0$．否则，即如果S中存在有限个元素 $x_1,\cdots,x_n(n\geqslant 1)$，$R$中存在不全为0的元素 $r_1,\cdots,r_n$，使得 $r_1x_1+\cdots+r_nx_n=0$，则称集合S是 **R-线性相关**的．

定义 S叫作是R-模M的一组**基**(或叫 **R-基**)，是指：

(1) S是R-线性无关的；并且

(2) S生成R-模M．

条件(2)相当于说，M中元素均可表成S中有限个元素的R-线性组合．而条件(1)相当于说，M中元素的这种表法是唯一的．因此，如果S是R-模M的一组基，则M是循环模 $Rx(x\in S)$的直和，即$M=\bigoplus\limits_{x\in S} Rx$．

具有基的R-模叫作是**自由 R-模**．

每个自由R-模可以有许多组不同的基．但是与域上向量空间的情形一样，不同的基具有相同的势．

定理 4 设R是具有幺元素的交换环，S和T是同一个自由R-模M的两组基．则$|T|=|S|$．

证明 如果S是有限集合，则由于T是一组基，从而S中每个元素均可表成T中有限个元素的R-线性组合．因为S有限，可知存在T的一个有限子集合T_0，使得S中每个元素均可表成T_0中元素的R-线性组合．但是S是M的一组R-基，从而M中每个元

素均可表成 T_0 中元素的 R-线性集合. 特别地，如果 $T-T_0\neq\emptyset$，则 $T-T_0$ 中元素也可表成 T_0 中元素的 R-线性组合. 但这是不可能的，因为 T 是线性无关集合. 从而 $T=T_0$，即 T 也是有限集. 这就证明了：S 和 T 或者同时为有限集，或者同时为无限集.

(1) 假设 S 和 T 同时是有限集合. 令 $S=\{x_1,\cdots,x_n\}$，$T=\{y_1,\cdots,y_m\}$. 如果 $n\neq m$，不妨设 $n>m$. 由于 S 是一组基，从而每个 y_i 可表成 $x_1,\cdots,x_n$ 的线性组合，即

$$y_i=\sum_{j=1}^{n}\alpha_{ij}x_j,\quad \alpha_{ij}\in R,1\leqslant i\leqslant m.$$

同样地也有

$$x_j=\sum_{k=1}^{m}\beta_{jk}y_k,\quad \beta_{jk}\in R,\ 1\leqslant j\leqslant n.$$

从而

$$\begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix}=BA\begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix}\qquad B=(\beta_{jk})_{n\times m},\quad A=(\alpha_{ij})_{m\times n}.$$

由表达式的唯一性可知 $BA=I_n$（n 阶单位方阵）. 由于 $n>m$，我们将 B 补上 $n-m$ 列 0，而将 A 补上 $n-m$ 行 0，均凑成 n 阶方阵，则有

$$(B\ 0)\begin{pmatrix}A\\ 0\end{pmatrix}=I_n.$$

两边取行列式，得到 $0\cdot 0=1$，这就得出矛盾. 因此必然 $|S|=n=m=|T|$.

(2) 假设 S 和 T 同时是无限集合，以 $K(T)$ 表示 T 的全部有限子集合而组成的集族. 我们如下方式构作映射 $f:S\to K(T)$. 办法是：对每个元素 $x\in S$，由于 T 是一组基，从而 $x=r_1y_1+\cdots+r_ny_n$，$r_i\in R$，$y_i\in T(1\leqslant i\leqslant n)$. 如果我们再要求 $r_1,\cdots,r_n$ 均不为 0（如果 $r_i=0$，则去掉 r_iy_i 这一项），那末 T 的有限子集$\{y_1,$

$\cdots,y_n\}\in K(T)$ 是由 x 所唯一决定的．于是我们定义 $f(x)=\{y_1,\cdots,y_n\}$．注意映射 $f:S\to K(T)$一般不是单射．但是

(i) 对每个 $T_0\in I_m f\subseteq K(T)$，$f^{-1}(T_0)$均是 S 的有限子集．这是因为：如果 $x\in f^{-1}(T_0)$，则 x 可表成 T_0 中元素的 R-线性组合，从而$f^{-1}(T_0)$包含在M的子模$M_{T_0}=\bigoplus_{y\in T_0}Ry$之中．而象本证明一开始所论述的，存在 S 的有限子集合 S_0，使得$M_{T_0}\subseteq M_{S_0}=\bigoplus_{x\in S_0}Rx$．从而 $f^{-1}(T_0)\subseteq M_{S_0}$．于是$f^{-1}(T_0)\subseteq S_0$．即 $f^{-1}(T_0)$是 S 的有限子集．

(ii) $\mathrm{Im}\,f$ 是 $K(T)$的无限子集．因为如果 $\mathrm{Im}\,f$ 是$K(T)$的有限子集，则 $T'=\bigcup_{T_0\in \mathrm{Im}\,f}T_0$ 为 T 的有限子集，而每个元素 $x\in S$均可表成 T' 中元素的R-线性组合．从而M中每个元素也均可表成 T' 中元素的 R-线性组合．于是$\bigoplus_{y\in T}Ry=M=\bigoplus_{y\in T'}Ry$．即 $T=T'$．但是T 为无限集合，而 T' 是 T 的有限子集．这一矛盾表明 $\mathrm{Im}\,f$ 是$K(T)$的无限子集．

现在我们构作另一个映射 $g:S\to \mathrm{Im}\,f\times\mathbf{N}$ （$\mathbf{N}$ 为自然数集合）．办法是：对每个 $x\in S$，令$f(x)=T_0\in\mathrm{Im}\,f$，则 $x\in f^{-1}(T_0)$．我们事先将每个有限集合 $f^{-1}(\tilde{T})(\tilde{T}\in\mathrm{Im}\,f)$中元素均排定一个次序．设 $f^{-1}(T_0)=\{x_1,\cdots,x_n\}$，如果 $x=x_k$，则定义 $g(x)=(T_0,k)\in\mathrm{Im}\,f\times\mathbf{N}$．由此定义的映射$g$是单射．于是$|S|\leqslant|\mathrm{Im}\,f|\cdot|\mathbf{N}|=|\mathrm{Im}\,f|\leqslant|T|$（这里用到了(ii)中证明的 $\mathrm{Im}\,f$ 是无限集这一事实）．完全对称地可证得$|T|\leqslant|S|$．从而$|T|=|S|$．这就完全证明了定理 4. ▌

注记 我们在定理的证明中，对于T和S均有限的情形利用了R是具有幺元素的交换环这一假定．因为在这种环上有通常的行列式理论．如果R不是交换环，我们也可以定义环R上的左（或右）模．这时，对于基的势无限的情形，定理 4 仍旧成立，并且这里给出的证明仍然有效．而对于基的势有限的情形，则定理 4 一般

不再成立．对于哪些非交换环使得定理4仍然成立，则是代数中一个有兴趣的问题．

根据定理4，如果M是具有幺元素的交换环R上的自由模，则M的任意一组基S的势是模M本身的特性而与S的取法无关．我们将$|S|$叫作是自由R-模M的**秩**，表示成$\mathrm{rank}_R M$．当R为域时，它就是R-向量空间M的维数$\dim_R M$．

设M是秩有限的自由R-模．$\mathrm{rank}_R M=n$．$\{x_1,\cdots,x_n\}$是M的一组基，则$M=\bigoplus\limits_{i=1}^{n}Rx_i$．但是我们有$R$-模同构

$$Rx_i \xrightarrow{\sim} R,\ ax_i\mapsto a \qquad (a\in R).$$

（这显然是R-模满同态，由于x_i是一个基元素，可知这也是单射．从而为同构．）因此$M\cong R\oplus\cdots\oplus R$（$n$个）$=R^n$．所以通常我们把秩为$n$的自由$R$-模记成$R^n$．

自由模的一个重要作用在于

引理 2 每个R-模M均同构于某个自由R-模的商模．并且，M是有限生成R-模$\Longleftrightarrow M$同构于秩有限的自由R-模的商模．

证明 取M的一组生成元S（例如总可取$S=M$），构作一个新的集合$\{x_i\,|\,i\in S\}$和自由R-模$\bigoplus\limits_{i\in S}Rx_i$，其中$Rx_i=\{rx_i\,|\,r\in R\}$．并且规定$rx_i=sx_i(r,s\in R)\Longleftrightarrow r=s$．定义$rx_i+sx_i=(r+s)x_i$，$r(sx_i)=(rs)x_i$．于是$Rx_i$成为$R$-模．作映射

$$f:\bigoplus_{i\in S}Rx_i\to M,\quad f(r_1x_{s_1}+\cdots+r_nx_{s_n})=r_1s_1+\cdots+r_ns_n,$$
$$r_i\in R,\ s_i\in S$$

这显然是R-模满同态．由同态基本定理可知$M\cong\bigoplus\limits_{i\in S}Rx_i/\mathrm{Ker}f$，即$M$同构于自由$R$-模的商模．

如果M是有限生成R-模，则可取生成元集合S为有限集．于是$\bigoplus\limits_{i\in S}Rx_i$的秩有限．即有限生成$R$-模同构于秩有限的自由模的商模．反之，若$M$同构于秩有限的自由模的商模，即存在

着R-模同构$f:\left(\bigoplus_{i=1}^{n} Rx_i\right)\Big/P\simeq M$，则$f(\bar{x}_1),\cdots,f(\bar{x}_n)$生成$R$-模$M$，即$M$是有限生成$R$-模. ▌

下一个引理是很重要的.

引理 3(中山引理) 设M是有限生成R-模，$\mathfrak{a}$是R的理想，并且$\mathfrak{a}\subseteq r(R)$($R$的大根). 如果$\mathfrak{a}M=M$，则$M=(0)$.

证明 以n表示生成R-模M的最少非零元素个数.如果$n\geqslant 1$，并且$M=Ru_1+\cdots+Ru_n$，$u_i\neq 0$，则$u_n\in M=\mathfrak{a}M$. 于是

$$u_n=a_1u_1+\cdots+a_nu_n \qquad (a_i\in\mathfrak{a},1\leqslant i\leqslant n),$$

从而$(1-a_n)u_n=a_1u_1+\cdots+a_{n-1}u_{n-1}$. 由于$a_n\in\mathfrak{a}\subseteq r(R)$，可知$1-a_n$为环$R$中单位(第一章定理5). 从而$u_n=(1-a_n)^{-1}a_1u_1+\cdots+(1-a_n)^{-1}a_{n-1}u_{n-1}$. 这表明$u_1,\cdots,u_{n-1}$生成$R$-模$M$. 这就与$n$的最小性相矛盾. 于是$n=0$，即$M=(0)$. ▌

引理 4 设M为有限生成R-模，N是M的R-子模. $\mathfrak{a}$是R的理想并且$\mathfrak{a}\subseteq r(R)$. 如果$M=\mathfrak{a}M+N$，则$M=N$.

证明 将中山引理用于有限生成R-商模M/N. 由于$\mathfrak{a}(M/N)=(\mathfrak{a}M+N)/N=M/N$. 从而$M/N=(0)$，即$M=N$. ▌

作为引理4的一个应用，我们现在介绍局部环上有限生成模的一个结果.设$(R,\mathfrak{m})$为局部环，$k=R/\mathfrak{m}$.如果M是R-模，则$\mathfrak{m}$将R-商模$M/\mathfrak{m}M$零化(即$\mathfrak{m}\cdot M/\mathfrak{m}M=(0)$)，从而$M/\mathfrak{m}M$可看成是域$k=R/\mathfrak{m}$上的向量空间. 如果$M$为有限生成$R$-模，则$M/\mathfrak{m}M$是有限维的$k$-向量空间.下面引理5表明我们可以由$M/\mathfrak{m}M$的一组基来决定$R$-模$M$的一组生成元.

引理 5 设$(R,\mathfrak{m})$为局部环，$k=R/\mathfrak{m}$，M为有限生成R-模.

(1) 如果 $x_1\cdots,x_n\in M$,并且$M/\mathrm{m}M=k\bar{x}_1\oplus\cdots\oplus k\bar{x}_n$，其中 $\bar{x}_i$ 表示 x_i 在$M/\mathrm{m}M$中的象,则$M=Rx_1+\cdots+Rx_n$.

(2) 如果M是秩有限的自由 R-模，则 $\mathrm{rank}_R M=\dim_k M/\mathrm{m}M$.

证明(1) 令$N=Rx_1+\cdots+Rx_n$,这是M的 R-子模. 由引理条件可知映射 $N\to M/\mathrm{m}M$, $x\mapsto\bar{x}$ 是满射. 这就表明$N+\mathrm{m}M=M$. 因为对于局部环,$\mathrm{m}=r(R)$. 从而由引理 4 可知$M=N=Rx_1+\cdots+Rx_n$.

(2) 如果$M=Rx_1\oplus\cdots\oplus Rx_n$，则 $M/\mathrm{m}M=(Rx_1\oplus\cdots\oplus Rx_n)/\mathrm{m}x_1\oplus\cdots\oplus\mathrm{m}x_n\cong\bigoplus_{i=1}^{n}(Rx_i/\mathrm{m}x_i)=\bigoplus_{i=1}^{n}kx_i$. 从而 $\dim_k M/\mathrm{m}M=n=\mathrm{rank}_R M$. ▌

注记 我们知道，域上的有限生成模(向量空间)必然有一组基，即必然是自由模(习题 1). 但是局部环上的有限生成模不必是自由模. 例如$R=\mathbf{Z}/4\mathbf{Z}$为局部环，$M=\mathbf{Z}/2\mathbf{Z}$是有限生成 $\mathbf{Z}/4\mathbf{Z}$-模. 但不是自由 $\mathbf{Z}/4\mathbf{Z}$-模. 因为一个有限生成自由 $\mathbf{Z}/4\mathbf{Z}$-模的元素个数为 4 的幂,而$M=\mathbf{Z}/2\mathbf{Z}$ 只有两个元素.

习 题

1. 域 k 上有限生成模M均是自由模，并且 $\dim_k M$ 等于M中 k-线性无关集合的最大势.

2. (1) 如果R为整环,则自由R-模M一定是无扭模. 试问无扭模是否一定为自由模?[提示:考虑$R=k[x,y]$. k 为域，而M为R中由 x,y 生成的理想作为R-模.]

(2) 如果不假定R为整环,则自由R-模是否一定为无扭R-模?

3. 设F为自由R-模,$g:A\to B$为R-模满同态. 则对于每个R-模同态$f:F\to B$,均有唯一的R-模同态$h:F\to A$,使得$f=gh$.

4. 设R为整环而M为秩有限的自由R-模. 则M中R-线性无关集合的最大势为 $\mathrm{rank}_R M$.

5．设R为任意具有幺元素的交换环，M为秩 n 的自由R-模．如果$M=Rx_1+\cdots+Rx_n$，求证$M=Rx_1\oplus\cdots\oplus Rx_n$．

6．自由模的子模或商模是否一定为自由模？有限生成模的子模和商模是否一定是有限生成模？

7．设M为秩 n 自由R-模，求证 $\mathrm{Hom}_R(M,R)$也是秩 n 自由R-模．

8．设M为有限生成R-模，X是M的子集并且X生成R-模M，求证X必有某个有限子集X_0，使得X_0生成R-模M．

§ 2.3 正合序列与交换图表

在模论中，我们不仅研究某个具体R-模的特性，更重要的是通过模同态研究不同模之间的联系．在研究各种不同的模和它们之间的同态联系的时候，经常使用两种基本的表达符号，这就是正合序列和交换图表．

定义 设R为环．R-模与R-模同态序列

$$M\xrightarrow{f}N\xrightarrow{g}P$$

叫作在N处正合，是指$\mathrm{Im}f=\mathrm{Ker}g$．这时，该序列也称作是正合的．一般地，$R$-模和$R$-模同态序列

$$M_0\xrightarrow{f_1}M_1\xrightarrow{f_2}M_2\xrightarrow{f_3}\cdots\xrightarrow{f_n}M_n$$

叫作是正合的，是指此序列在$M_1,M_2,\cdots,M_{n-1}$处均正合，即$\mathrm{Im}f_i=\mathrm{Ker}f_{i+1}$ $(1\leqslant i\leqslant n-1)$．

例如：

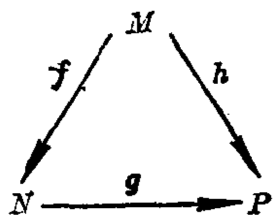
(1) 模序列$0\xrightarrow{i}M\xrightarrow{f}N$正合（为简单起见今后也用0表示零模(0)），相当于说f是单同态．这是因为i只能是零同态（因此i通常可略去不写），从而此序列正合$\Longleftrightarrow\mathrm{Ker}f=\mathrm{Im}i=(0)\Longleftrightarrow f$为单同态．

(2) 模序列$M\xrightarrow{f}N\xrightarrow{p}0$正合相当于说$f$是满同态．这是由于$p$只能是零同态（从而$p$通常也略去不写），于是此序列正合$\Longleftrightarrow\mathrm{Im}f=\mathrm{Ker}p=N\Longleftrightarrow f$是满同态．

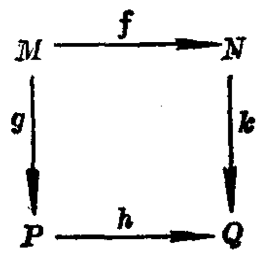
(3) 模序列 $0\to N\xrightarrow{f}M\xrightarrow{g}P\to 0$ 正合相当于说 $N\cong f(N)=\mathrm{Im}f=\mathrm{Ker}g$,并且 $g(M)=P$. 从而由同态定理得到$P\cong M/\mathrm{Im}f$. 特别若N是M的子模,而 $i:N\to M$ 为包含映射(即对每个 $x\in N$, 令$i(x)=x\in M$),则由同态定理可知,正合序列 $0\to N\xrightarrow{i}M\xrightarrow{g}P\to 0$ 相当于模同构$M/N\overset{\bar g}{\simeq}P$,其中$\bar g(\bar x)=g(x)(x\in M)$.

形如 $0\to N\xrightarrow{f}M\xrightarrow{g}P\to 0$ 的正合序列叫作**短正合序列.**

定义 由 R-模和 R-模同态组成的图表



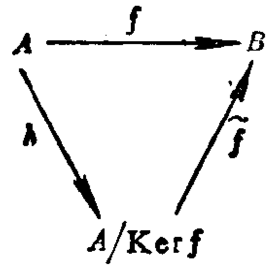
叫作是**交换的**,是指 $gf=h$. 这也相当于说,对于M中每个元素 x, 均有 $h(x)=g(f(x))$, 即 x 经过图表中两条不同的路线映成 P中同一元素. 类似地,图表



叫作是交换的,是指$kf=hg$. 一个更复杂的图表叫作是交换的,是指:若图表中从模M到模N有两条不同的路线,则M中每个元素经这两条不同线路映成模 N的同一个元素.

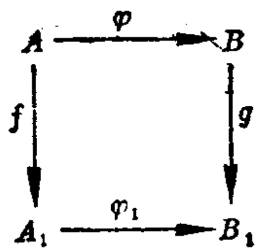
例如:

(1) 设 $f:A\to B$是R-模同态, $\tilde f:A/\mathrm{Ker}f\to B$为由$f$ 诱导的R-模单同态, $h:A\to A/\mathrm{Ker}f$是标准满同态(即$\tilde f(\bar a)=f(a)\in B$, $h(a)=\bar a$, 对于$a\in A$). 则图表



是交换的．这个交换图表形象地表示出任意一个模同态 f 如何自然地分解成一个满同态 h 和一个单同态 $\tilde{f}$ 之连续作用．

(2) 考虑R-模和R-模同态图表



如果这个图表是交换的，则

(i) $\varphi(\mathrm{Ker}f)\subseteq\mathrm{Ker}g$．(这是由于：若 $a\in\mathrm{Ker}f$，则 $g\varphi(a)=\varphi_1 f(a)=\varphi_1(0)=0$，从而 $\varphi(a)\in\mathrm{Ker}g$.)于是，我们得到 R-模同态

$$\varphi':\mathrm{Ker}f\to\mathrm{Ker}g,\varphi'=\varphi|_{\mathrm{Ker}f}(\text{即}\varphi\text{在}\mathrm{Ker}f\text{上的限制}).$$

(ii) $\varphi_1(\mathrm{Im}f)\subseteq\mathrm{Im}g$．(这是由于：若$a_1\in\mathrm{Im}f$，则有$a\in A$使得$a_1=f(a)$．从而$\varphi_1(a_1)=\varphi_1 f(a)=g\varphi(a)\in\mathrm{Im}g$.)于是，对于由$\varphi_1$诱导出的自然同态$\tilde{\varphi}_1:A_1\to B_1/\mathrm{Im}g$，$\tilde{\varphi}_1(a_1)=\overline{\varphi_1(a_1)}$，我们有$\mathrm{Im}f\subseteq\mathrm{Ker}\tilde{\varphi}_1$．从而又诱导出新的$R$-模同态

$$\bar{\varphi}_1:A/\mathrm{Im}f\to B_1/\mathrm{Im}g,\qquad \bar{\varphi}_1(\bar{a}_1)=\overline{\varphi_1(a_1)}.$$

引理 6 假设由R-模和R-模同态组成的图表

$$\begin{array}{ccccccc} & & A & \xrightarrow{\varphi} & B & \xrightarrow{\psi} & C & \to 0 \\ & & \downarrow f & & \downarrow g & & \downarrow h & \\ 0 & \to & A_1 & \xrightarrow{\varphi_1} & B_1 & \xrightarrow{\psi_1} & C_1 & \end{array} \qquad (\Delta)$$

是交换的,并且图表中的两个行均是正合序列. 则

(1) $\mathrm{Ker} f \xrightarrow{\varphi'} \mathrm{Ker}\, g \xrightarrow{\psi'} \mathrm{Ker} h$ 正合.

(2) $A_1/\mathrm{Im}\, f \xrightarrow{\overline{\varphi}_1} B_1/\mathrm{Im}\, g \xrightarrow{\psi_1} C_1/\mathrm{Im} h$ 正合.

证明 (1) 由于图表(Δ)的第一行正合,从而$\psi\varphi(A)=\psi(\mathrm{Im}\varphi)=\psi(\mathrm{Ker}\psi)=0$,即$\psi\varphi=0$ (零同态),因此$\psi'\varphi'=\psi\varphi|_{\mathrm{Ker} f}=0$.即 $\mathrm{Im}\varphi'\subseteq\mathrm{Ker}\psi'$. 只需再证 $\mathrm{Im}\varphi'\supseteq\mathrm{Ker}\psi'$.设$b\in\mathrm{Ker}\, g$ 并且$b\in\mathrm{Ker}\psi'$,则$\psi(b)=\psi'(b)=0$.由于图表(Δ)的第一行正合,可知$b\in\mathrm{Ker}\psi=\mathrm{Im}\,\varphi$,于是有 $a\in A$使得$\varphi(a)=b$. 但是 $\varphi_1 f(a)=g\varphi(a)=g(b)=0$ (因为$b\in\mathrm{Ker}\, g$),而 φ_1 为单射(因为图表(Δ)的第二行正合),从而$f(a)=0$,即 $a\in\mathrm{Ker} f$, 而 $\varphi'(a)=\varphi(a)=b$. 即 $b\in\mathrm{Im}\varphi'$. 这就表明$\mathrm{Ker}\psi'\subseteq\mathrm{Im}\varphi'$.

(2) 同样,由 $\psi_1\varphi_1=0$ 得到$\overline{\psi}_1\overline{\varphi}_1=0$,即$\mathrm{Im}\overline{\varphi}_1\subseteq\mathrm{Ker}\overline{\psi}_1$ 只需再证$\mathrm{Im}\overline{\varphi}_1\supseteq\mathrm{Ker}\overline{\psi}_1$.假定 $b_1\in B_1$并且 $\overline{b}_1\in\mathrm{Ker}\overline{\psi}_1$,则$\overline{\psi_1(b)}=\overline{\psi}_1(\overline{b}_1)=\overline{0}$,从而$\overline{\psi_1(b_1)}\in\mathrm{Im} h$. 于是存在$c\in C$,使得$h(c)=\psi_1(b_1)$.由于$\psi$ 是满射,又存在$b\in B$使得$\psi(b)=c$.于是对于$b_1'=a_1-g(b)\in B_1$,我们有 $\overline{b}_1'=\overline{b}_1$ 并且 $\psi_1(b_1')=\psi_1(b_1)-\psi_1 g(b)=h(c)-h\psi(b)=h(c)-h(c)=0$.即$b_1'\in\mathrm{Ker}\psi_1=\mathrm{Im}\varphi_1$. 从而有$a_1\in A_1$使得$\varphi_1(a_1)=b_1'$. 于是$\overline{\varphi}_1(\overline{a}_1)=\overline{b}_1'=\overline{b}_1$. 即$\overline{b}_1\in\mathrm{Im}\overline{\varphi}_1$. 这就证明了$\mathrm{Im}\overline{\varphi}_1\supseteq\mathrm{Ker}\,\overline{\psi}_1$. ▌

注记 更为精彩的是,可以发现R-模同态$\delta:\mathrm{Ker} h\to A_1/\mathrm{Im} f$,使得长序列

$$\mathrm{Ker} f\xrightarrow{\varphi'}\mathrm{Ker}\, g\xrightarrow{\psi'}\mathrm{Ker} h\xrightarrow{\delta}A_1/\mathrm{Im} f\xrightarrow{\varphi_1}B_1/\mathrm{Im}\, g\xrightarrow{\psi_1}C_1/\mathrm{Im} h$$

是正合的, 这个结果称作是“蛇形引理”. 由于本书中不需要这部分内容,因此从略.

作为引理6的直接推论是

引理 7 在引理6的假定之下，

(1) 如果 f 和 h 均为单同态，则 g 也是单同态.

(2) 如果 f 和 h 均为满同态，则 g 也是满同态.

(3) 如果 f 和 h 均为同构，则 g 也是同构.

证明 (1) 由引理6的(1) 推出. 因为这时有正合序列 $0=\operatorname{Ker} f\xrightarrow{\varphi'}\operatorname{Ker} g\xrightarrow{\psi'}\operatorname{Ker} h=0$. 于是 $0=\varphi'(0)=\operatorname{Im}\varphi'=\operatorname{Ker}\psi'=\operatorname{Ker} g$. 即 g 为单同态.

(2) 如果 $\operatorname{Im} f=A_1$, $\operatorname{Im} h=C_1$，则由引理6的(2)有正合序列 $0=A_1/\operatorname{Im} f\to B_1/\operatorname{Im} g\to C_1/\operatorname{Im} h=0$，从而 $B_1/\operatorname{Im} g=(0)$，即 g 为满同态.

(3) 由(1) 和(2) 得出. ▌

定理 5 设 $0\to A_1\xrightarrow{f} B\xrightarrow{g} A_2\to 0$ 是 R-模和 R-模同态的短正合序列. 则下列三个条件彼此等价:

(1) 存在 R-模同态 $h: A_2\to B$，使得 $gh=1_{A_2}$;

(2) 存在 R-模同态 $k: B\to A_1$，使得 $kf=1_{A_1}$;

(3) 存在 R-模同构 $\varphi: A_1\oplus A_2\cong B$. 使得图表

$$\begin{array}{ccccccccc}
0 & \to & A_1 & \xrightarrow{i_1} & A_1\oplus A_2 & \xrightarrow{p_2} & A_2 & \to & 0\\
 & & \downarrow{\scriptstyle 1_{A_1}} & & \downarrow{\scriptstyle\varphi} & & \downarrow{\scriptstyle 1_{A_2}} & & \\
0 & \to & A_1 & \xrightarrow{f} & B & \xrightarrow{g} & A_2 & \to & 0
\end{array}$$

是交换的，其中 $i(a_1)=(a_1,0)$, $p_2(a_1,a_2)=a_2$ $(a_1\in A_1, a_2\in A_2)$.

证明 (1)⇒(3): 定义映射 $f\oplus h$: $A_1\oplus A_2\to B$, $(f\oplus h)(a_1, a_2)=f(a_1)+h(a_2)$. 易知这是 R-模同态. 考虑图表

$$\begin{array}{ccccccccc}
0 & \to & A_1 & \xrightarrow{i_1} & A_1\oplus A_2 & \xrightarrow{p_2} & A_2 & \to & 0\\
 & & \downarrow{\scriptstyle 1_{A_1}} & & \downarrow{\scriptstyle f\oplus h} & & \downarrow{\scriptstyle 1_{A_2}} & & \\
0 & \to & A_1 & \xrightarrow{f} & B & \xrightarrow{g} & A_2 & \to & 0
\end{array}$$

这个图表是交换的．因为左面四边形显然是交换的，而右面四边形的交换性是由于$gf=0$和$gh=1_{A_2}$，从而$g(f\oplus h)=gf\oplus gh=0\oplus 1_{A_2}=p_2=1_{A_2}p_2$．进而，图表的第二行已假定是正合的，而容易验证第一行也是正合的．于是由引理 7 可知$f\oplus h$事实上是R-模同构．取$\varphi=f\oplus h$即得到(3)的要求．

(2)⇒(3)：定义$\psi: B\to A_1\oplus A_2$，$\psi(b)=(k(b),g(b))$．这是R-模同态，并且图表

$$\begin{array}{ccccccccc}
0 & \to & A_1 & \xrightarrow{f} & B & \xrightarrow{g} & A_2 & \to & 0\\
 & & \downarrow{\scriptstyle 1_{A_1}} & & \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle 1_{A_2}} & & \\
0 & \to & A_1 & \xrightarrow{i_1} & A_1\oplus A_2 & \xrightarrow{p_2} & A_2 & \to & 0
\end{array}$$

是交换的（左面四边形的交换性是由于$gf=0$和$kf=1_{A_1}$，而右面四边形的交换性是显然的．）再由引理 7 即知ψ为同构．由此即知图表

$$\begin{array}{ccccccccc}
0 & \to & A_1 & \xrightarrow{i_1} & A_1\oplus A_2 & \xrightarrow{p_2} & A_2 & \to & 0\\
 & & \downarrow{\scriptstyle 1_{A_1}} & & \downarrow{\scriptstyle \psi^{-1}} & & \downarrow{\scriptstyle 1_{A_2}} & & \\
0 & \to & A_1 & \xrightarrow{f} & B & \xrightarrow{g} & A_2 & \to & 0
\end{array}$$

也是交换的，即可取$\varphi=\psi^{-1}$．

(3)⇒(1)和(2)：由(3)的假定我们有交换图表

$$\begin{array}{ccccccccc}
0 & \to & A_1 & \xrightarrow{i_1} & A_1\oplus A_2 & \xrightarrow{p_2} & A_2 & \to & 0\\
 & & \downarrow{\scriptstyle 1} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle 1} & & \\
0 & \to & A_1 & \xrightarrow{f} & B & \xrightarrow{g} & A_2 & \to & 0
\end{array}$$

定义$p_1: A_1\oplus A_2\to A_1$，$p_1(a_1,a_2)=a_1$，$i_2: A_2\to A_1\oplus A_2$，$i_2(a_2)=(0,a_2)$．则$p_1i_1=1_{A_1}$，$p_2i_2=1_{A_2}$．由此不难验证图表

$$\begin{array}{ccccc}
A_1 & \xleftarrow{p_1} & A_1\oplus A_2 & \xleftarrow{i_2} & A_2\\
\downarrow{\scriptstyle 1} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle 1}\\
A_1 & \xrightarrow{f} & B & \xrightarrow{g} & A_2
\end{array}$$

也是交换的．定义 $h=\varphi i_2: A_2\to B$ 和 $k=p_1\varphi^{-1}: B\to A_1$，利用这个新图表的交换性即知 $gh=1_{A_2}, kf=1_{A_1}$．∎

定义 满足定理 5 中条件的短正合序列 $0\to A_1\xrightarrow{f} B\xrightarrow{g} A_2\to 0$ 叫作是**分裂的**．

显然，对于分裂的短正合序列，我们有 R-模同构 $B\cong A_1\oplus A_2$，但是，短正合序列即使 $B\cong A_1\oplus A_2$ 也不必是分裂的．

习　　题

1．设 $0\to V_1\to V_2\to\cdots\to V_n\to 0$ 为域 k 上有限维向量空间和 k-线性变换的正合序列，求证：

$$\sum_{i=1}^{n}(-1)^i\dim_k V_i=0.$$

2．设 R 为整环，$T(M)$ 表示 R-模 M 的扭子模．

(1) 若 $f: A\to B$ 为 R-模同态，则 $f(T(A))\subseteq T(B)$．

我们以 $T(f)=f|_{T(A)}$ 表示 f 在 $T(A)$ 上的限制．

(2) 如果 $0\to A\xrightarrow{f} B\xrightarrow{g} C$ 是 R-模正合序列，求证 $0\to T(A)\xrightarrow{T(f)} T(B)\xrightarrow{T(g)} T(C)$ 也是 R-模正合序列．

(3) 如果 $B\xrightarrow{g} C\to 0$ 为正合序列，试问 $T(B)\xrightarrow{T(g)} T(C)\to 0$ 是否一定正合？

3．（五项引理）设 R-模图表

$$\begin{array}{ccccccccc}
A_1 & \xrightarrow{f_1} & A_2 & \xrightarrow{f_2} & A_3 & \xrightarrow{f_3} & A_4 & \xrightarrow{f_4} & A_5 \\
\downarrow{\scriptstyle\alpha_1} & & \downarrow{\scriptstyle\alpha_2} & & \downarrow{\scriptstyle\alpha_3} & & \downarrow{\scriptstyle\alpha_4} & & \downarrow{\scriptstyle\alpha_5} \\
B_1 & \xrightarrow{g_1} & B_2 & \xrightarrow{g_2} & B_3 & \xrightarrow{g_3} & B_4 & \xrightarrow{g_4} & B_5
\end{array}$$

是交换的，并且两行均是正合的．求证：

(1) 如果 α_1 为满同态，α_2 和 α_4 为单同态，则 α_3 为单同态。[提示：利用短正合序列 $0\to A_2/\mathrm{Ker}f_2\xrightarrow{\bar{f}_2}A_3\xrightarrow{f_3}\mathrm{I_m}f_3\to 0$]

(2) 如果 α_5 为单同态，α_2 和 α_4 为满同态，则 α_3 为满同态。

4．求证：R-模短正合序列 $0\to A_1\xrightarrow{f}B\xrightarrow{g}A_2\to 0$ 是分裂的 $\Longleftrightarrow f(A_1)$ 是 R-模 B 的直和成分，即存在 B 的 R-子模 C，使得 $B=f(A_1)\oplus C$。

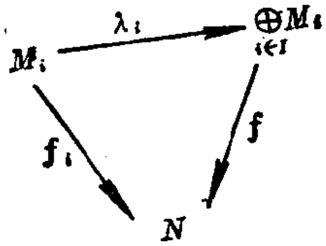
5．假设 R-模图表

$$\begin{array}{ccccccc}
A_1 & \xrightarrow{f_1} & A_2 & \xrightarrow{f_2} & \cdots & \xrightarrow{f_{n-1}} & A_n \\
\downarrow{\scriptstyle h_1} & & \downarrow{\scriptstyle h_2} & & \cdots & & \downarrow{\scriptstyle h_n} \\
B_1 & \xrightarrow{g_1} & B_2 & \xrightarrow{g_2} & \cdots & \xrightarrow{g_{n-1}} & B_n
\end{array}$$

是交换的，并且 $h_1,\cdots,h_n$ 均是 R-模同构。如果图表中两个行序列之中的一个是正合的，则另一个也是正合的。

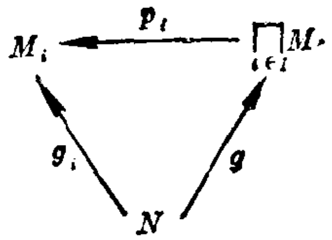
6．设 $M_i(i\in I)$是一个 R-模族，N 为 R-模。求证：

(1) 如果 $f_i:M_i\to N$ 均是 R-模同态，则存在唯一的 R-模同态 f: $\bigoplus\limits_{i\in I}M\to N$，使得对每个 $i\in I$，图表



都是交换的。其中 λ_i 是 M_i 到$\bigoplus\limits_{i\in I}M_i$ 的标准嵌入，即对于 $m\in M_i$，$\lambda_i(m)=(m_j)_{j\in I}\in\bigoplus\limits_{i\in I}M_i$，其中 $m_i=m$，而 $j\neq i$ 时 $m_j=0$。

(2) 如果 $g_i:N\to M_i$ 均是 R-模同态，则存在唯一的 R-模同态 $g:N\to\prod\limits_{I\in i}M_i$，使得对每个 $i\in I$，图表



都是交换的，其中 p_i 是 $\prod_{i\in I}M_i$ 到 M_i 的标准投射，即 $p_i((m_i)_{i\in I})=m_i$。

（3）求证有 R-模同构：$\mathrm{Hom}_R(\bigoplus_{i\in I}M_i,N)\cong\prod_{i\in I}\mathrm{Hom}_R(M_i,N)$，

$$\mathrm{Hom}_R(N,\prod_{i\in I}M_i)\cong\prod_{i\in I}\mathrm{Hom}_R(N,M_i).$$

§ 2.4 同态算子 Hom，投射模

模的正合序列和交换图表不过是反映出一些模之间的良好的联系．从已知的正合序列和交换图表构造出新的正合序列和交换图表这一形式化过程，反映出人们从某些模之间的已知的联系发现出新的联系．例如引理 6 即是这方面的例子（而引理 6 后面注记中所述的蛇形引理则是更精彩的例子）．由已知正合序列构作新正合序列的最基本方法有两个，即采用同态算子 Hom 和张量积算子$\otimes$，本节谈 Hom．

设 $\varphi:A\to B$ 为 R-模同态．对于每个 R-模同态 $g:D\to A$，我们得到一个同态 $\varphi g:D\to B$．从而给出一个映射

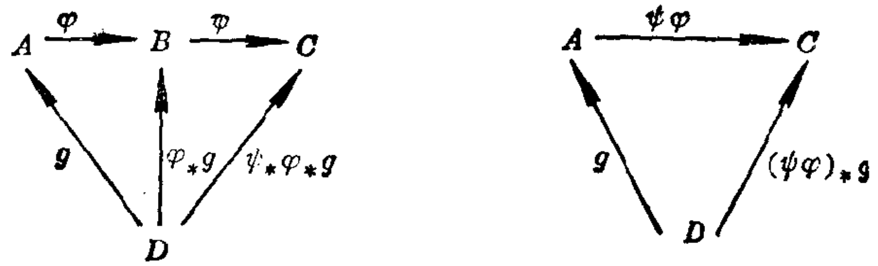
$$\varphi_*:\mathrm{Hom}_R(D,A)\to\mathrm{Hom}_R(D,B),\quad \varphi_*(g)=\varphi g.$$

对于我们在§2.1 中所定义的 $\mathrm{Hom}_R(D,A)$ 和 $Hom_R(D,B)$ 的 R-模结构，不难验证 φ_* 也是 R-模同态（这需要验证 $\varphi(g\pm g')=\varphi g\pm\varphi g'$ 和 $\varphi(rg)=r(\varphi g)$），并且

（1）当 $\varphi=1_A:A\to A$ 时，$(1_A)_*=1_{\mathrm{Hom}_R(D,A)}$．

（2）如果又有 R-模同态 $\psi:B\to C$，则 $(\psi\varphi)_*=\psi_*\varphi_*$．比如说，对于每个 $g\in\mathrm{Hom}_R(D,A)$，均有 $(\psi\varphi)_*g=\psi\varphi g=\psi(\varphi_*g)=\psi_*\varphi_*g$，从而 $(\psi\varphi)_*=\psi_*\varphi_*$．或者由于下面两个交换图表是同一

件事情也可证得此等式.



定理 6 R-模序列$\mathscr{E}$：$0\to A\xrightarrow{\varphi}B\xrightarrow{\psi}C$是正合的$\Longleftrightarrow$对于每个$R$-模$D$，$R$-模序列

$\mathrm{Hom}(D,\mathscr{E})$：$0\to\mathrm{Hom}_R(D,A)\xrightarrow{\varphi_*}\mathrm{Hom}_R(D,B)\xrightarrow{\psi_*}\mathrm{Hom}_R(D,C)$
都是正合的.

证明 $\Rightarrow$：(1)先证序列$\mathrm{Hom}(D,\mathscr{E})$在$\mathrm{Hom}_R(D,A)$处的正合性.也就是要证$\mathrm{Ker}\varphi_*=0$. 设$f\in\mathrm{Hom}_R(D,A)$，$f\in\mathrm{Ker}\varphi_*$，则$\varphi f=0$. 从而对每个$x\in D$均有$\varphi f(x)=0\in B$. 但是$\varphi$为单射，于是$f(x)=0$（对每个$x\in D$），即$f=0$. 这就表明$\mathrm{Ker}\varphi_*=0$.

(2) 再证$\mathrm{Im}\varphi_*\subseteq\mathrm{Ker}\psi_*$，这相当于证明$\psi_*\varphi_*=0$. 而这是容易的，因为$\psi_*\varphi_*=(\psi\varphi)_*=(0)_*=0$.

(3) 最后证$\mathrm{Im}\varphi_*\supseteq\mathrm{Ker}\psi_*$.设$g\in\mathrm{Hom}_R(D,B)$，$g\in\mathrm{Ker}\psi_*$.则$\psi g=0$.从而$\mathrm{Im}\,g\subseteq\mathrm{Ker}\psi=\mathrm{Im}\varphi$.由于$\varphi$为单同态，可知$\varphi$: $A\to\mathrm{Im}\varphi$为同构. 令$h\in\mathrm{Hom}_R(D,A)$表示合成同态$D\xrightarrow{g}\mathrm{Im}\,g\xrightarrow{i}\mathrm{Im}\,\varphi\xrightarrow{\varphi^{-1}}A$，其中$i$为包含映射. 则$g=\varphi h=\varphi_*(h)$. 因此$g\in\mathrm{Im}\varphi_*$. 于是$\mathrm{Im}\varphi_*\supseteq\mathrm{Ker}\psi_*$.

由(2) 和(3) 即知序列$\mathrm{Hom}(D,\mathscr{E})$在$\mathrm{Hom}_R(D,B)$处正合.

$\Leftarrow$：我们选取恰当的D以证明序列$\mathscr{E}$的正合性.

(1) 取$D=\mathrm{Ker}\varphi$，i: $D\to A$为包含映射. 则$\varphi_*(i)=\varphi i=0$. 由于φ_*是单射，可知$i=0$. 于是$D=0$，即$\mathrm{Ker}\varphi=0$. 从而序列$\mathscr{E}$在A

处正合.

(2) 取$D=A$. 由于$\mathrm{Ker}\psi_*=\mathrm{Im}\varphi_*$, 从而$0=\psi_*\varphi_*(1_A)=\psi\varphi 1_A=\psi\varphi$. 因此$\mathrm{Im}\varphi\subseteq\mathrm{Ker}\psi$.

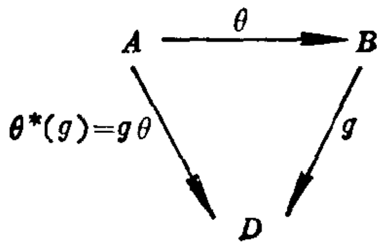
(3) 最后取$D=\mathrm{Ker}\psi$, $j:D\to B$为包含映射. 由于$0=\psi j=\psi_*(j)$, 并且$\mathrm{Ker}\psi_*=\mathrm{Im}\varphi_*$, 可知存在$f\in\mathrm{Hom}_R(D,A)$使得$j=\varphi_*(f)=\varphi f$. 于是对每个$x\in D=\mathrm{Ker}\psi$, 均有$x=j(x)=\varphi f(x)\in\mathrm{Im}\varphi$. 从而$\mathrm{Ker}\psi\subseteq\mathrm{Im}\varphi$.

由(2)和(3)即知序列$\mathscr{E}$在B处正合. ▌

类似地, 设$\theta:A\to B$是R-模同态. 对于每个$f\in\mathrm{Hom}_R(B,D)$, $f\theta\in\mathrm{Hom}_R(A,D)$. 于是我们得到映射

$$\theta^*:\mathrm{Hom}_R(B,D)\to\mathrm{Hom}_R(A,D),\theta^*(f)=f\theta.$$

这个映射可以用下面的交换图表显示出来



θ^*是R-模同态, 并且

(1) $(1_B)^*=1_{\mathrm{Hom}_R(B,D)}$.

(2) 如果又有R-模同态$\zeta:B\to C$,则$(\zeta\theta)^*=\theta^*\zeta^*$. (因为对每个$g\in\mathrm{Hom}_R(C,D)$,$(\zeta\theta)^*g=g\zeta\theta=(\zeta^*g)\theta=\theta^*\zeta^*g$.)

定理 7 R-模序列$\mathscr{E}:A\xrightarrow{\theta}B\xrightarrow{\zeta}C\longrightarrow 0$正合$\Longleftrightarrow$对于每个$R$-模$D$, R-模序列

$$\mathrm{Hom}(\mathscr{E},D):0\to\mathrm{Hom}_R(C,D)\xrightarrow{\zeta^*}\mathrm{Hom}_R(B,D)\xrightarrow{\theta^*}\mathrm{Hom}_R(A,D)$$

均正合.

证明 $\Rightarrow$：$\mathrm{Ker}\zeta^*=0$ 和 $\theta^*\zeta^*=0$ 的证明与定理 6 相仿. 我们只需再证 $\mathrm{Im}\zeta^*\supseteq\mathrm{Ker}\theta^*$. 假设 $f\in\mathrm{Hom}_R(B,D)$，$f\in\mathrm{Ker}\theta^*$，则 $0=\theta^*(f)=f\theta$. 于是 $0=f(\mathrm{Im}\theta)=f(\mathrm{Ker}\zeta)$ 由此诱导出 R-模同态

$$\bar{f}:B/\mathrm{Ker}\zeta\to D,\bar{f}(\bar{b})=f(b)\quad(b\in B).$$

由正合序列$\mathscr{E}$和同态基本定理可知我们还有 R-模同构

$$\bar{\zeta}:B/\mathrm{Ker}\zeta\simeq C,\bar{\zeta}(\bar{b})=\zeta(b)\quad(b\in B).$$

于是给出 R-模同态 $\bar{f}\bar{\zeta}^{-1}:C\to D$. 绘出交换图表可验证$\zeta^*(\bar{f}\bar{\zeta}^{-1})=f$. 从而 $f\in\mathrm{Im}\zeta^*$，即 $\mathrm{Im}\zeta^*\supseteq\mathrm{Ker}\theta^*$.

$\Leftarrow$：(1) 取 $D=C/\mathrm{Im}\zeta$，$p:C\to D$ 为标准满同态，则 $\zeta^*(p)=p\zeta=0$. 但是 ζ^* 为单射，从而 $p=0$，即 $C=\mathrm{Im}\zeta$. 从而序列$\mathscr{E}$在C处正合.

(2) 取 $D=B/\mathrm{Im}\theta$，$p:B\to D$ 为标准满同态，则$\theta^*(p)=p\theta=0$. 于是 $p\in\mathrm{Ker}\theta^*=\mathrm{Im}\zeta^*$. 即存在 $f\in\mathrm{Hom}_R(C,D)$，使得 $p=\zeta^*(f)=f\zeta$. 从而 $p(\mathrm{Ker}\zeta)=f\zeta(\mathrm{Ker}\zeta)=0$. 这就表明 $\mathrm{Ker}\zeta\subseteq\mathrm{Im}\theta$.

(3) 最后取 $D=C$，则 $0=\theta^*\zeta^*(1_C)=\zeta\theta$. 于是 $\mathrm{Im}\theta\subseteq\mathrm{Ker}\zeta$. 这就完全证明了序列$\mathscr{E}$是正合的. ▌

注记 我们可以把定理 6 和定理 7 的"$\Rightarrow$"部分简略地说成是：同态算子 $\mathrm{Hom}_R(\ \ ,D)$和 $\mathrm{Hom}_R(D,\ \ )$均是**左正合算子**. 这意味着，它们把正合序列$\mathscr{E}$作用成正合序列 $\mathrm{Hom}_R(\mathscr{E},D)$和 $\mathrm{Hom}_R(D,\mathscr{E})$，而后两个序列均是左边从 0 开始的序列. 一般来说，对于任意的 R-模 D，我们不能保证 $\mathrm{Hom}_R(\ \ ,D)$和 $\mathrm{Hom}_R(D,\ \ )$具有右正合性质. 也就是说：

(1) 如果 $B\xrightarrow{\psi}C\to0$ 是 R-模正合序列，则 $\mathrm{Hom}_R(D,B)\xrightarrow{\psi_*}\mathrm{Hom}_R(D,C)\to0$ 不必正合. 例如取 $R=\mathbf{Z}$，则有 $\mathbf{Z}$-模(即 Abel 群)正合序列 $\mathbf{Z}\xrightarrow{p}\mathbf{Z}/2\mathbf{Z}\to0$，其中 p 为正则满同态. 但是对 $D=\mathbf{Z}/2\mathbf{Z}$，我们有 $\mathrm{Hom}(\mathbf{Z}/2\mathbf{Z},\mathbf{Z})=0$，$\mathrm{Hom}(\mathbf{Z}/2\mathbf{Z},\mathbf{Z}/2\mathbf{Z})$是 2

阶群．从而

$$\begin{array}{ccc}\mathrm{Hom}(\mathbf{Z}/2\mathbf{Z},\mathbf{Z}) & \xrightarrow{p_*} & \mathrm{Hom}(\mathbf{Z}/2\mathbf{Z},\mathbf{Z}/2\mathbf{Z})\to 0 \\ \| & & \not\| \\ 0 & & 0\end{array}$$

不可能是正合序列．

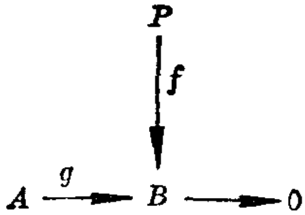
(2) 同样地，若 $0\to A\xrightarrow{\theta}B$ 为 R-模正合序列，则 $\mathrm{Hom}_R(B,D)\xrightarrow{\theta^*}\mathrm{Hom}_R(A,D)\to 0$ 也不必正合．例如考虑 $\mathbf{Z}$-模正合序列 $0\to\mathbf{Z}\xrightarrow{i}\mathbf{Q}$ 和 $D=\mathbf{Z}$（其中 i 为包含映射，$\mathbf{Q}$ 是有理数加法群），则

$$\begin{array}{ccc}\mathrm{Hom}(\mathbf{Q},\mathbf{Z}) & \to & \mathrm{Hom}(\mathbf{Z},\mathbf{Z})\to 0 \\ \| & & \not\| \\ 0 & & 0\end{array}$$

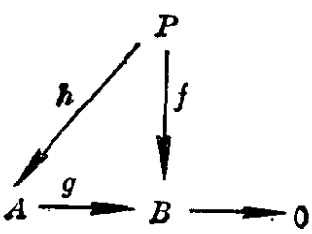
不正合．

现在自然要提出这样的问题：设 R 是一个固定的环，对于何种 R-模 P，由 R-模序列 $A\xrightarrow{g}B\to 0$ 的正合性一定能推得序列 $\mathrm{Hom}_R(P,A)\xrightarrow{g^*}\mathrm{Hom}_R(P,B)\to 0$ 的正合性？这就是说，如果 $g:A\to B$ 为 R-模满同态，则希望 g_* 也是 R-模满同态，即对于每个 $f\in\mathrm{Hom}_R(P,B)$，均有 $h\in\mathrm{Hom}_R(P,A)$，使得 $f=g_*(h)=gh$．或者用图表的语言叙述成：

对于每个 R-模图表



如果行序列是正合的，则必然存在 $h\in\mathrm{Hom}_R(P,A)$，使得图表



是交换的.

定义 满足上述条件的 R-模 P 叫作是投射 R-模.

投射模在近代数学中起着不小的作用. 现在我们给出它的另一些刻画方式.

定理 8 设 P 为 R-模,则下列条件彼此等价.

(1) P 是投射 R-模.

(2) 如果 $A\xrightarrow{f}B\to 0$ 是 R-模正合序列, 则 $\mathrm{Hom}_R(P,A)\xrightarrow{f_*}\mathrm{Hom}_R(P,B)\to 0$ 也是 R-模正合序列.

(3) 如果 $0\to A\xrightarrow{\varphi}B\xrightarrow{\psi}C\to 0$ 是 R-模短正合序列, 则 $0\to\mathrm{Hom}_R(P,A)\xrightarrow{\varphi_*}\mathrm{Hom}_R(P,B)\xrightarrow{\psi_*}\mathrm{Hom}_R(P,C)\to 0$ 是 R-模短正合序列.

(4) 每个 R-模短正合序列 $0\to A\xrightarrow{f}B\xrightarrow{g}P\to 0$ 必分裂.

(5) P 是自由 R-模的直和成分, 即存在自由 R-模 F 和 R-模 K,使得 $F\cong P\oplus K$.

证明 (1) $\Longleftrightarrow$(2):如投射模定义之前所述.

(2) $\Longleftrightarrow$(3):由定理 6(Hom的左正合性)和(2)即得到(3). 反之, 如果(3)成立, 并且 $A\xrightarrow{f}B\to 0$ 正合, 则我们有短正合序列 $0\to\mathrm{Ker}\,f\xrightarrow{i}A\xrightarrow{f}B\to 0$, 其中 i 是包含映射. 于是由 (3) 得到短正合序列 $0\to\mathrm{Hom}_R(P,\mathrm{Ker}f)\to\mathrm{Hom}_R(P,A)\xrightarrow{f_*}\mathrm{Hom}_R(P,B)\to 0$. 特别地, 它的一部分 $\mathrm{Hom}_R(P,A)\xrightarrow{f_*}\mathrm{Hom}_R(P,B)\to 0$ 是正合的. 这就证明了(2).

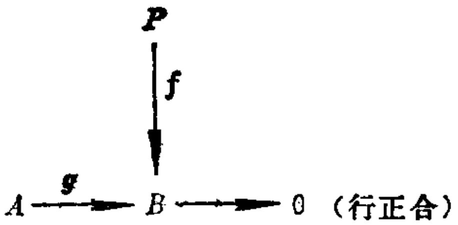
(1)$\Rightarrow$(4):根据投射模的定义, 对于图表

$$\begin{array}{ccccc} & & P & & \\ & & \downarrow{\scriptstyle 1_P} & & \\ B & \xrightarrow{g} & P & \longrightarrow & 0 \end{array}\quad(\text{行正合})$$

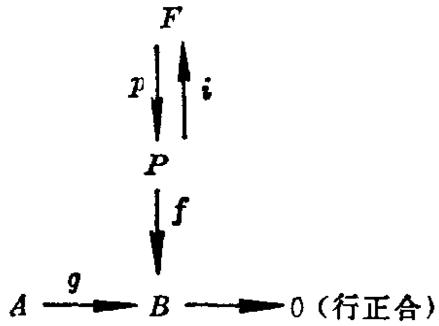
存在 R-模同态 $h:P\to B$，使得 $gh=1_P$. 由定理 5 即知短正合序列 $0\to A\xrightarrow{f}B\xrightarrow{g}P\to 0$ 必然分裂.

(4)⇒(5)：根据引理 2，每个模均是自由模的商模. 从而存在自由 R-模 F 和 F 的 R-子模 K，使得 $0\to K\xrightarrow{i}F\to P\to 0$ 是正合序列. 由(4)推出此正合序列是分裂的. 特别地我们得到 $F\cong P\oplus K$（定理 5 的(3)）.

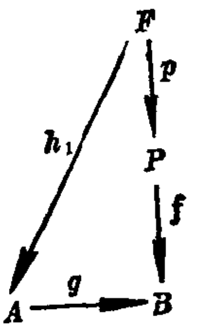
(5)⇒(1)：对于图表



令 p 为合成同态 $F\simeq K\oplus P\xrightarrow{p_2}P$，$i$ 为合成同态 $P\xrightarrow{i_2}K\oplus P\simeq F$，其中 $p_2(x,y)=y$，$i_2(y)=(0,y)$. 于是把上面的图表扩大成



对于自由模 F，我们知道存在 R-模同态 $h_1:F\to A$，使得图表

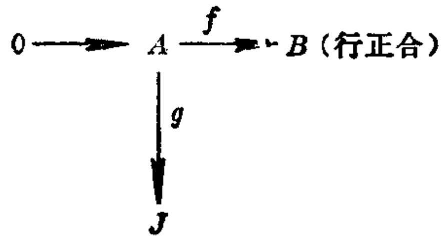


是交换的（§ 2.2 的习题 3）. 令 $h=h_1i\in \mathrm{Hom}_R(P,A)$，则 $gh=$

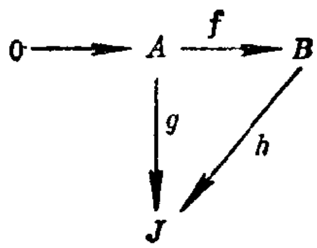
$gh_1i=fpi=f1_P=f$. 从而 h 即为所求. ∎

类似于投射模的定义，我们有

定义 设 J 为 R-模. 如果对于 R-模图表



必有 $h\in \mathrm{Hom}_R(B,J)$，使得图表



是交换的，则称 J 为**内射 R-模**.

定理 8′ 设 J 为 R-模，则以下诸条件彼此等价：

(1) J 是内射 R-模.

(2) 若 $0\to A\xrightarrow{f}B$ 是 R-模正合序列，则 $\mathrm{Hom}_R(B,J)\xrightarrow{f^*}\mathrm{Hom}_R(A,J)\to 0$ 也是 R-模正合序列.

(3) 若 $0\to A\xrightarrow{f}B\xrightarrow{g}C\to 0$ 是 R-模短正合序列，则 $0\to\mathrm{Hom}_R(C,J)\xrightarrow{g^*}\mathrm{Hom}_R(B,J)\xrightarrow{f^*}\mathrm{Hom}_R(A,J)\to 0$ 是 R-模短正合序列.

(4) 每个 R-模短正合序列 $0\to J\to B\to C\to 0$ 都是分裂的.

(5) 若 J 为某个 R-模 B 的子模，则 J 必是 B 的直和成分.

证明 由于本书不用内射模的知识，故证明从略. 但对于读

者却是熟悉和运用正合序列和交换图表的一个很好的练习. ▍

由定理 8 的(5)(或者由§2.2 的习题 3)可知自由模必为投射模，但是反之不然. 例如，我们有 $\mathbf{Z}/6\mathbf{Z}$-模同构 $\mathbf{Z}/6\mathbf{Z}\cong \mathbf{Z}/2\mathbf{Z}\oplus \mathbf{Z}/3\mathbf{Z}$. 从而 $\mathbf{Z}/2\mathbf{Z}$ 和 $\mathbf{Z}/3\mathbf{Z}$ 均是投射 $\mathbf{Z}/6\mathbf{Z}$-模. 但它们显然均不是自由 $\mathbf{Z}/6\mathbf{Z}$-模. 不过在许多方面，投射模可看成是自由模的一种推广. 并且对于某些特殊类型的环 R，有限生成投射 R-模必然是自由 R-模. 比如说

定理 9 局部环(R,m)上的有限生成投射模必是自由模.

证明 设 P 是有限生成投影 R-模. 于是有 R-模满同态 $\pi: F\to P$，其中 $F=\bigoplus_{i=1}^{n}Rx_i$. 令 n 是满足这些条件的最小自然数. 这时 $P=R\pi(x_1)+\cdots+R\pi(x_n)$. 令 $K=\mathrm{Ker}\pi$. 我们先证明 $K\subseteq \mathrm{m}F$. 假如 $k\in K, k\notin \mathrm{m}F$，则当 k 唯一地表示成 $k=r_1x_1+\cdots+r_nx_n(r_i\in R)$的时候，必然有某个 r_i 不属于m. 不妨设 $r_1\notin \mathrm{m}$，则$r_1\in U(R)$. 从而 $x_1-r_1^{-1}k=-r_1^{-1}(r_2x_2+\cdots+r_nx_n)$. 将此式作用 π，即得到 $\pi(x_1)=\sum_{i=2}^{n}-r_1^{-1}r_i\pi(x_i)$. 这表明 $P=R\pi(x_2)+\cdots+R\pi(x_n)$. 令 $F'=\bigoplus_{i=2}^{n}Rx_i$，而 $\pi':F'\to P$ 是 π 在 F的子模F'上的限制. 由上面所述可知 π' 也是满同态. 这就与 n 的极小性相矛盾. 因此 $K\subseteq \mathrm{m}F$.

现在 $0\to K\xrightarrow{i}F\xrightarrow{\pi}P\to 0$ 是 R-模正合序列. 由于 P 是投射模，从而这个短正合序列是分裂的. 于是 $F=K\oplus P'$, $P'\cong P$. 从而 $F=K\oplus P'\subseteq \mathrm{m}F+P'\subseteq F$. 即 $F=\mathrm{m}F+P'$. 从而 $\mathrm{m}(F/P')=(\mathrm{m}F+P')/P'=F/P'$. 由于 F/P'是有限生成 R-模. 利用中山引理可知 $F/P'=0$. 即 $P'=F$. 从而 $P\cong F$. 于是 P 为自由 R 模. ▍

我们在§ 2.6 中还要证明(作为定理 12(A)的直接推论)，如果 R 为主理想整环，则有限生成投射 R-模也必为自由模.

习　　题

1. 证明定理 8′.

2. 设 $P_j(j\in J)$ 均为 R-模，求证：$\bigoplus_{j\in J} P_j$ 为投射 R-模 $\Longleftrightarrow P_j(j\in J)$ 均为投射 R-模.

3. 求证下列三条件彼此等价：

(1) $\mathscr{E}$：$0\to A\overset{\varphi}{\to}B\overset{\psi}{\to}C\to 0$ 是分裂的短正合 R-模序列.

(2) 对于每个 R-模 D，$\mathrm{Hom}(D,\mathscr{E})$：$0\to \mathrm{Hom}_R(D,A)\overset{\varphi_*}{\to}\mathrm{Hom}_R(D,B)\overset{\psi_*}{\to}\mathrm{Hom}_R(D,C)\to 0$ 均是分裂的短正合序列.

(3) 对于每个 R-模 D，$\mathrm{Hom}(\mathscr{E},D)$：$0\to \mathrm{Hom}_R(C,D)\overset{\psi^*}{\to}\mathrm{Hom}_R(B,D)\overset{\varphi^*}{\to}\mathrm{Hom}_R(A,D)\to 0$ 均是分裂的短正合序列.

[提示：(1)⇒(3)：由序列 $\mathscr{E}$ 的分裂性可知有同态 $\alpha:B\to A$，使得 $\alpha\varphi=1_A$. 试验证 $\varphi^*\alpha^*=1_{\mathrm{Hom}_R(A,D)}$. 从而 φ^* 为满同态. 于是 $\mathrm{Hom}(\mathscr{E},D)$ 为短正合序列. 并且由 $\varphi^*\alpha^*=1$ 知此短正合序列是分裂的. (3)⇒(1)：取 $D=A$. 由于 φ^* 为满射可知有 $f\in\mathrm{Hom}_R(B,A)$，使得 $1_A=\varphi^*(f)=f\varphi$. 从而 φ 为单射，于是 $\mathscr{E}$ 为短正合序列. 再由 $f\varphi=1_A$ 可知 $\mathscr{E}$ 是分裂的. 类似地证明(1)⟺(2).]

4. 设 P 是有限生成投射 R-模，则 $\mathrm{Hom}_R(P,R)$ 也是有限生成投射 R-模.

5. 设 $A\overset{f}{\to}B\overset{g}{\to}C\to 0$ 是 R-模正合序列. 则：C 为投射 R-模 $\Longleftrightarrow$ 存在 R-模同态 $h:B\to A$，使得 $fhf=f$.

6. 设 M 为 R-模，$M^*=\mathrm{Hom}_R(M,R)$，$M^{**}=\mathrm{Hom}_R(\mathrm{Hom}_R(M,R),R)$. 对于 $a\in M$，定义 $\varphi_a:\mathrm{Hom}_R(M,R)\to R$，$f\mapsto f(a)$.

(1) 求证 $\varphi:M\to M^{**}$，$a\mapsto\varphi_a$ 是 R-模同态.

(2) 如果 M 是自由 R-模，则 φ 是单同态.

(3) 如果 M 是有限生成投射 R-模，则 $\varphi:M\to M^{**}$ 是 R-模同构.

§ 2.5 张量积算子⊗，平坦模

现在我们介绍用来产生新正合序列的第二个重要的算子：张量积算子．先谈什么是模的张量积．

设 A 和 B 均为 R-模．令 F 是以集合 $A\times B$ 为基的自由 Abel 群．考虑 F 的如下子集合

$$\left\{\begin{matrix}(a+a',b)-(a,b)-(a',b)\\(a,b+b')-(a,b)-(a,b')\\(ra,b)-(a,rb)\end{matrix}\ \middle|\ a,a'\in A,b,b'\in B,r\in R\right\}.$$

以 S 表示由这个子集合所生成的 F 的子群．我们把 Abel 商群 F/S 叫作是 R-模 A 和 B 的**张量积**，表示成 $A\otimes_R B$．(当 $R=\mathbf{Z}$ 时，$\otimes_{\mathbf{Z}}$ 简记为 $\otimes$．)而其中元素 $\overline{(a,b)}$ 记为 $a\otimes b$，叫作是元素 $a\in A$ 和 $b\in B$ 的张量积．由定义可知，$A\otimes_R B$ 中每个元素均可表示成 $\sum\limits_{i=1}^{n}a_i\otimes b_i(a_i\in A,b_i\in B)$．但是表法不是唯一的，因为有如下的关系：

$$\begin{aligned}&(a+a')\otimes b=a\otimes b+a'\otimes b,\\&a\otimes(b+b')=a\otimes b+a\otimes b' \qquad (a,a'\in A,b,b'\in B,r\in R),\\&(ra)\otimes b=a\otimes(rb).\end{aligned}$$

如果我们再定义

$$r(a\otimes b)=(ra)\otimes b(=a\otimes(rb)) \qquad (r\in R,a\in A,b\in B),$$

然后把这个乘 r 运算线性地扩充到 $A\otimes_R B$ 的全部元素上，即

$$r\left(\sum_{i=1}^{n}a_i\otimes b_i\right)=\sum_{i=1}^{n}r(a_i\otimes b_i).$$

可以直接验证，$A\otimes_R B$ 由此可成为 R-模．

定义 设 A,B,C 均为 R-模．映射 $f:A\times B\to C$ 叫作是 **R-**

双线性的，是指对于任意 $a,a'\in A,b,b'\in B$ 和 $r\in R$ 均有

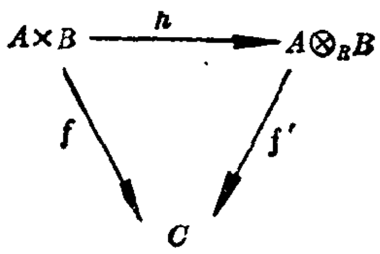
$$f(a+a',b)=f(a,b)+f(a',b),$$

$$f(a,b+b')=f(a,b)+f(a,b'),$$

$$rf(a,b)=f(ra,b)=f(a,rb).$$

例如，映射 $f:A\times B\to A\otimes_R B$，$f(a,b)=a\otimes b$ 就是 R-双线性映射．我们现在要证明张量积 $A\otimes_R B$ 对于 R-双线性映射具有所谓“泛性质”．确切说来就是

定理 10(张量积的泛性质)　设 A，B 和 C 均是 R-模．$h: A\times B\to A\otimes_R B$ 为标准映射，即 $h(a,b)=a\otimes b$．则对于每个 R-双线性映射 $f:A\times B\to C$，均有唯一的 R-模同态 $f':A\otimes_R B\to C$，使得 $f=f'h$．即(集合和映射的)图表



是交换的．

证明　由于 $A\times B$ 是自由 Abel 群 F 的基，从而映射 f 以唯一的方式扩充成 Abel 群同态 $\tilde{f}:F\to C$，即 $\tilde{f}\left(\sum_{i=1}^{n}(a_i,b_i)\right)=\sum_{i=1}^{n}f(a_i,b_i)$．而由 f 的 R-双线性可知子群 S 包含在 $\operatorname{Ker}\tilde{f}$ 之中．于是诱导出 Abel 群同态 $f':F/S=A\otimes_R B\to C$．可以直接验证 f' 事实上为 R-模同态(这是由于 $rf(a,b)=f(ra,b)$)，并且 $f=f'h$．最后，f' 的唯一性是由于：如果 $f=f'h$，则 $f'(a\otimes b)$ 必然为 $f(a,b)$．而 f' 由此唯一决定，因为 $A\otimes_R B$ 是由 $\{a\otimes b\mid a\in A,b\in B\}$ 所生成的．▌

利用张量积的泛性质，可以证明关于张量积的许多结果.

引理 8 设 A,A_i,B,C 均为 R-模，则有如下的 R-模同构：

(1) $A\otimes_R B\cong B\otimes_R A$.

(2) $R\otimes_R A\cong A$.

(3) $(\bigoplus\limits_{i\in I}A_i)\otimes_R B\cong\bigoplus\limits_{i\in I}(A_i\otimes_R B)$.

(4) $(A\otimes_R B)\otimes_R C\cong A\otimes_R(B\otimes_R C)$.

证明 (1) 考虑映射 $f:A\times B\to B\otimes_R A,f(a,b)=b\otimes a$. 这是 R-双线性映射(例如$f(a+a',b)=b\otimes(a+a')=b\otimes a+b\otimes a'=f(a,b)+f(a',b)$等等). 于是由定理 10 得到 R-模同态 $f':A\otimes_R B\to B\otimes_R A$，使得 $f'(a\otimes b)=b\otimes a$. 类似地，我们有 R-模同态 $g':B\otimes_R A\to A\otimes_R B$，使得 $g'(b\otimes a)=a\otimes b$. 显然 $f'g'=1_{B\otimes A}$，$g'f'=1_{A\otimes B}$. 从而 f' 是 R-模同构. 即 $A\otimes_R B\cong B\otimes_R A$.

(2) 考虑映射 $R\times A\to A$，$(r,a)\mapsto ra$. 这是 R-双线性映射，从而诱导出 R-模同态 $f:R\otimes_R A\to A$，使得 $f(r\otimes a)=ra$. 另一方面，考虑映射 $g:A\to R\otimes_R A,g(a)=1\otimes a$. 这显然是 R-模同态. 并且 $fg=1_A(fg(a)=f(1\otimes a)=1.a=a)$，$gf=1_{R\otimes A}$ $(gf(r\otimes a)=g(ra)=1\otimes ra=(r\cdot 1)\otimes a=r\otimes a)$. 从而 $R\otimes_R A\cong A$.

(3) 设 $i_k:A_k\to\bigoplus\limits_{i\in I}A_i$ 为标准嵌入，即将 $a_k\in A_k$ 映成 $\bigoplus\limits_{i\in I}A_i$ 中这样的元素：它的第 k 分量为 a_k，而其余分量均为 0. 又设 $p_k:\bigoplus\limits_{i\in I}A_i\to A_k$ 为标准投射，即 $p_k((a_i)_{i\in I})=a_k$. 它们均是 R-模同态，并且

$$(*)\quad p_k i_l=0\ (k\neq l\text{ 时}),p_k i_k=1_{A_k},\sum_{k\in I}i_k p_k=1_{\oplus A_i}.$$

定义映射

$$\alpha:\bigoplus_{i\in I}(A_i\otimes_R B)\to(\bigoplus_{i\in I}A_i)\otimes_R B.$$

它是由 $\alpha((a_i\otimes b)_{i\in I})=\sum\limits_{i\in I}(i_i(a_i)\otimes b)=(\sum\limits_{i\in I}i_i(a_i))\otimes b$(这是有限和)经线性扩充而成的映射. 这是 R-模同态. 另一方面，映射 $(\bigoplus\limits_{i\in I}A_i)\times B\to\bigoplus\limits_{i\in I}(A_i\otimes_R B)$，$(u,b)\mapsto(p_i(u)\otimes b)_{i\in I}$ 是 R-双线性

映射，于是诱导出 R-模同态

$$\beta:(\bigoplus_{i\in I}A_i)\otimes_R B\to\bigoplus_{i\in I}(A_i\otimes_R B).$$

使得 $\beta(u\otimes b)=(p_i(u)\otimes b)_{i\in I}$. 利用关系式（$*$）可知 α 和 β 互逆. 从而均是 R-模同构.

（4）证明留给读者作练习. ▌

设 A,A',B,B' 均是 R-模. $f:A\to B, f':A'\to B'$ 为 R-模同构. 定义映射

$$A\times A'\to B\otimes_R B',(a,a')\mapsto f(a)\otimes f'(a').$$

这是 R-双线性映射，从而诱导出唯一的 R-模同态

$$f\otimes f':A\otimes_R A'\to B\otimes_R B',$$

使得 $(f\otimes f')(a\otimes a')=f(a)\otimes f'(a')$. 并且如果又有 R-模同态 $g:B\to C$ 和 $g':B'\to C'$，易知有

$$(g\otimes g')(f\otimes f')=(gf\otimes g'f').$$

定理 11 下列诸条件彼此等价：

（1）$\mathscr{E}$：$A\xrightarrow{f}B\xrightarrow{g}C\to 0$ 为 R-模正合序列.

（2）对于每个 R-模 D,

$$D\otimes\mathscr{E}:\ D\otimes_R A\xrightarrow{1\otimes f}D\otimes_R B\xrightarrow{1\otimes g}D\otimes_R C\to 0$$

均是 R-模正合序列.

（3）对于每个 R-模 D,

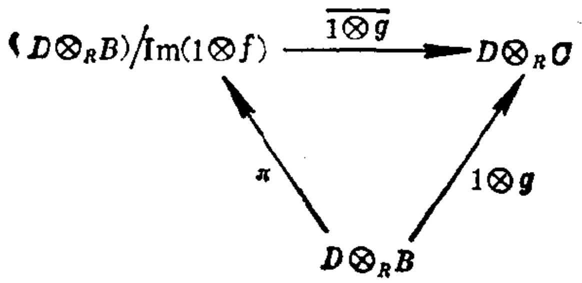
$$\mathscr{E}\otimes D:\ A\otimes_R D\xrightarrow{f\otimes 1}B\otimes_R D\xrightarrow{g\otimes 1}C\otimes_R D\to 0$$

均是 R-模正合序列.

证明 （1）$\Rightarrow$（2）：为证序列 $D\otimes\mathscr{E}$ 在 $D\otimes_R C$ 处的正合性，只需证 $\mathrm{Im}(1\otimes g)=D\otimes_R C$. 这由 g 的满射性不难得到. 因为对每个 $c\in C$ 均有 $b\in B$ 使 $c=g(b)$. 从而对每个 $d\in D$ 均有 $(1\otimes g)(d\otimes b)=d\otimes c$. 而 $D\otimes_R C$ 是由 $\{d\otimes c\mid d\in D,c\in C\}$ 生成的，所以 $\mathrm{Im}(1\otimes g)=D\otimes_R C$.

由 $gf=0$ 可知 $(1\otimes g)(1\otimes f)=1\otimes gf=1\otimes 0=0$，从而 $\mathrm{Im}(1\otimes f)\subseteq\mathrm{Ker}(1\otimes g)$.

最后证 $\mathrm{Im}(1\otimes f)=\mathrm{Ker}(1\otimes g)$：由 $\mathrm{Im}(1\otimes f)\subseteq\mathrm{Ker}(1\otimes g)$ 可知 $1\otimes g$ 诱导出 R-模同态 $\overline{1\otimes g}$：$(D\otimes_R B)/\mathrm{Im}(1\otimes f)\to D\otimes_R C$. 从而有交换图表



其中 π 为标准满同态. 我们只需再证 $\overline{1\otimes g}$ 是 R-模同构即可. 因为由此便得到 $\mathrm{Ker}(1\otimes g)=\mathrm{Ker}(\overline{1\otimes g}\cdot\pi)=\mathrm{Ker}\,\pi=\mathrm{Im}(1\otimes f)$.

考虑映射 $\varphi: D\times C\to(D\otimes_R B)/\mathrm{Im}(1\otimes f)$，$(d,c)\mapsto\overline{d\otimes b}$，其中 b 满足 $g(b)=c$. 这个映射是可以定义的. 因为若又有 $g(b')=c$，则 $b-b'\in\mathrm{Ker}\,g=\mathrm{Im}\,f$，从而 $\overline{d\otimes b}=\overline{d\otimes b'}$. 易知 φ 为 R-双线性映射. 于是诱导出 R-模同态

$$\bar{\varphi}: D\otimes_R C\to(D\otimes_R B)/\mathrm{Im}(1\otimes f),$$

使得 $\bar{\varphi}(d\otimes c)=\overline{d\otimes b}$，其中 $\varphi(b)=c$. 验证 $\bar{\varphi}$ 和 $\overline{1\otimes g}$ 互逆. 从而 $\overline{1\otimes g}$ 为 R-模同构. 这就证明了 $D\otimes\mathscr{E}$ 是正合序列.

(2)⇒(1)：由引理 8 给出了 R-模同构 $h_A: A\simeq R\otimes_R A$，$h_A(a)=1\otimes a$. 类似地定义 h_B 和 h_C. 可直接验证图表

$$\begin{array}{ccccccc}
A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 0\\
\downarrow h_A & & \downarrow h_B & & \downarrow h_C & & \\
R\otimes_R A & \xrightarrow{1\otimes f} & R\otimes_R B & \xrightarrow{1\otimes g} & R\otimes_R C & \longrightarrow & 0
\end{array}$$

是交换的. 由(2)知第二行正合(取 $D=R$)，从而第一行也正合(§2.3 习题 5).

(2)⟺(3)：对于任意模 D，我们在引理 8 中给出了 R-模同

构 $h_A: A\otimes_R D\cong D\otimes_R A$，$h_A(a\otimes d)=d\otimes a$. 类似地定义 h_B 和 h_C. 可直接验证图表

$$\begin{array}{ccccccc} A\otimes_R D & \xrightarrow{f\otimes 1} & B\otimes_R D & \xrightarrow{g\otimes 1} & C\otimes_R D & \longrightarrow & 0 \\ \downarrow h_A & & \downarrow h_B & & \downarrow h_C & & \\ D\otimes_R A & \xrightarrow{1\otimes f} & D\otimes_R B & \xrightarrow{1\otimes g} & D\otimes_R C & \longrightarrow & 0 \end{array}$$

是交换的，于是由此图表中的一个行是正合的，可推出另一行也是正合的. 这就表明(2)和(3)是等价的. ▌

注记 1. 定理11可以简单地说成：张量积算子 $D\otimes_R$ 和 $\otimes_R D$ 均是右正合算子.

2. 如果 $0\to A\xrightarrow{f} B$ 是 R-模正合序列，对每个 R-模 D，$0\to D\otimes_R A\xrightarrow{1\otimes f} D\otimes_R B$（或者等价地，$0\to A\otimes_R D\xrightarrow{f\otimes 1} B\otimes_R D$）是否也一定正合？答案一般是否定的. 例如 $0\to \mathbf{Z}\xrightarrow{i}\mathbf{Q}$ 是正合 $\mathbf{Z}$-模序列（其中 i 为包含映射）. 取 $D=\mathbf{Z}/2\mathbf{Z}$，则 $\mathbf{Z}/2\mathbf{Z}\otimes\mathbf{Z}\cong\mathbf{Z}/2\mathbf{Z}$（引理8），$\mathbf{Z}/2\mathbf{Z}\otimes\mathbf{Q}=0$（习题2）. 从而

$$\begin{array}{ccccc} 0\to & \mathbf{Z}/2\mathbf{Z}\otimes\mathbf{Z} & \to & \mathbf{Z}/2\mathbf{Z}\otimes\mathbf{Q} & \text{不正合.} \\ & \not\parallel & & \parallel & \\ & 0 & & 0 & \end{array}$$

定义 R-模 D 叫作是**平坦 R-模**，是指：若 $0\to A\xrightarrow{f} B$ 为 R-模正合序列，则 $0\to A\otimes_R D\xrightarrow{f\otimes 1} B\otimes_R D$（或者等价地：$0\to D\otimes_R A\xrightarrow{1\otimes f} D\otimes_R B$）也必为正合序列.

由定理11可知，这也相当于：若 $0\to A\xrightarrow{f} B\xrightarrow{g} C\to 0$ 为 R-模短正合序列，则 $0\to A\otimes_R D\xrightarrow{f\otimes 1} B\otimes_R D\xrightarrow{g\otimes 1} C\otimes_R D\to 0$（或者等价地：$0\to D\otimes_R A\xrightarrow{1\otimes f} D\otimes_R B\xrightarrow{1\otimes g} D\otimes_R C\to 0$）也必为短正合的. 这也可以简单地说成：$D$ 为平坦 R-模的充要条件是张量积算子 $\otimes_R D$（或 $D\otimes_R$）是正合算子.

下面是平坦模的性质.

引理 9 (1) R为平坦R-模.

(2) 设$B_i(i\in I)$均为R-模,则$\bigotimes_{i\in I}B_i$为平坦R-模$\Longleftrightarrow B_i(i\in I)$均为平坦$R$-模.

(3) 投射R-模必为平坦R-模.

证明 (1) 设$f:A\to B$是R-模同态. 我们有交换图表

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ h_A\downarrow & & \downarrow h_B \\ R\otimes_R A & \xrightarrow{1\otimes f} & R\otimes_R B \end{array}$$

其中h_A和h_B是自然的R-模同构. 于是由f为单射可得到$1\otimes f$为单射. 这就表明R是平坦R-模.

(2) 首先我们指出一个明显的事实: 如果$\{f_i:A_i\to A_i'\}_{i\in I}$为一个$R$-模同态族,则有唯一的$R$-模同态$\oplus f_i:\bigoplus_{i\in I}A_i\to\bigoplus_{i\in I}A_i'$,使得$(a_i)_{i\in I}\mapsto(f_i(a_i))_{i\in I}$. 并且$\oplus f_i$为单射$\Longleftrightarrow f_i(i\in I)$均为单射.

现在设$f:A\to A'$是R-模单同态,则有交换图表

$$\begin{array}{ccc} (\oplus B_i)\otimes_R A & \xrightarrow{1\otimes f} & (\oplus B_i)\otimes_R A' \\ \beta_A\downarrow & & \downarrow\beta_{A'} \\ \oplus(B_i\otimes_R A) & \xrightarrow{\oplus(1_i\otimes f)} & \oplus(B_i\otimes_R A') \end{array}$$

其中β_A和$\beta_{A'}$是引理 8 (3)的证明中给出的R-模同构, 即满足$\beta_A((b_i)_{i\in I}\otimes a)=(b_i\otimes a)_{i\in I}$. 由此交换图表可知

$1\otimes f$ 为单射$(1=1_{\oplus B_i})\Longleftrightarrow\oplus(1_i\otimes f)$为单射$(1_i=1_{B_i})$

$\Longleftrightarrow 1_i\otimes f(i\in I)$均为单射.

这就表明$\bigoplus_{i\in I}B_i$为平坦R-模$\Longleftrightarrow B_i(i\in I)$均为平坦$R$-模.

(3) 设P为投射R-模. 则 $F=P'\oplus K$, $P\cong P'$,其中F为自由R-模. 但是F同构于一些R的直和. 由(1)知R为平坦R-模. 从而由(2)可知自由R-模F也是平坦R-模. 于是同构于F的直和成分的P也是平坦R-模. ▌

系数环的扩张

设$f: R\to S$是环的同态.我们在§2.2例5中表明了一个S-模如何借助于f可成为R-模（$rx=f(r)x$, $r\in R$）. 现在我们利用张量积算子，借助于f可以把一个R-模作成S-模. 最常用于R是S的子环而f为包含映射的情形，这时相当于把一个R-模的系数环从R扩大成S，从而是系数环的扩张.

如果$f. R\to S$是环的同态，则S自然地看成是R-模.（对于$r\in R$, $s\in S$，定义$rs=f(r)s$.）于是对于每个R-模M，我们有张量积$S\otimes_R M$. 我们已经给出$S\oplus_R M$的R-模结构. 进一步，对于$s, s'\in S$, $m\in M$，定义$s'(s\otimes m)=(s's)\otimes m$. 然后将这种乘$S$中元素的运算线性地扩充到整个$S\otimes_R M$之上，容易验证$S\otimes_R M$由此而成为$S$-模. 从而系数环从$R$改成$S$.

例 设M为$\mathbf{Z}$-模（Abel群）$\mathbf{Z}\oplus\mathbf{Z}/n\mathbf{Z}$（$n\geqslant 1$）. 则$\mathbf{Q}\otimes M$为$\mathbf{Q}$上的向量空间. 事实上，

$$\begin{aligned}\mathbf{Q}\otimes M=\mathbf{Q}\otimes(\mathbf{Z}\oplus\mathbf{Z}/n\mathbf{Z})&\cong(\mathbf{Q}\otimes\mathbf{Z})\oplus(\mathbf{Q}\otimes\mathbf{Z}/n\mathbf{Z})\\&\cong\mathbf{Q}\oplus 0\cong\mathbf{Q}.\end{aligned}$$

从而$\mathbf{Q}\otimes\mathbf{M}$是$\mathbf{Q}$上的一维向量空间，它把$\mathbf{Z}$-模$M$的扭子模$T(M)=\mathbf{Z}/n\mathbf{Z}$“杀掉”. 我们在§2.6中要给出主理想整环$R$上任意有限生成模$M$的一般结构. 那时可以看出，如果令$K$是$R$的商域，则$K\otimes_R M$即是将$M$的扭子模$T(M)$杀掉，而变成$K$上的向量空间，并且$\dim_K(K\otimes_R M)=\operatorname{rank}_R M$（$=M$中$R$-线性无关元素个数的最大值）.

我们已经说过，$A\otimes_R B$中每个元素是有限个形如$a\otimes b$的元素之和. 但令人不愉快的是，这种表达式是不唯一的. 例如在$\mathbf{Z}\otimes\mathbf{Z}$中，$1\otimes 5=2\otimes 2+1\otimes 1$. 但是当$A$或$B$中有一个为自由$R$-模的时候，我们可以把$A\otimes_R B$中元素唯一地表达成某种形式.

引理 10 设F是以Y为基的自由R-模，即$F=\bigoplus_{y\in Y}Ry$. 而A

为任意 R-模. 则 $A\otimes_R F$ 中元素均可唯一地表示成 $\sum_{i=1}^{n} a_i\otimes y_i$，其中 $n\geqslant 0, 0\neq a_i\in A, y_i\in Y$，并且诸 $y_i(1\leqslant i\leqslant n)$ 两两不同.

证明 表达式的存在性是显然的. 为证唯一性，只需证明如果 $\sum_{i=1}^{n} a_i\otimes y_i=\sum_{i=1}^{n} b_i\otimes y_i$，其中 $a_i, b_i\in A$，$y_i\in Y$，并且诸 y_i $(1\leqslant i\leqslant n)$ 两两不同，则必然 $a_i=b_i(1\leqslant i\leqslant n)$.

记 $A_y=A\otimes_R Ry(y\in Y)$. 我们知道 $A_y\to A, a\otimes y\mapsto a$ 是 R-模同构，因此由 $a\otimes y=a'\otimes y$ 可推出 $a=a'$. 进而，我们在引理 8 中证明了

$$A\otimes_R F=A\otimes_R(\bigoplus_{y\in Y}Ry)\cong\bigoplus_{y\in Y}(A\otimes_R Ry)=\bigoplus_{y\in Y}A_y.$$

仔细考查那里给出的同构，可知元素 $\sum_{i=1}^{n} a_i\otimes y_i\in A\otimes_R F$ (诸 y_i 两两不同)映成元素 $\{t_y\}_{y\in Y}\in\bigoplus_{y\in Y}A_y$，其中 $\{t_y\}_{y\in Y}$ 的第 y_i 分量为 $t_{y_i}=a_i\otimes y_i(1\leqslant i\leqslant n)$，而对于其余的 $y, t_y=0$. 因此若 $\sum_{i=1}^{n} a_i\otimes y_i=\sum_{i=1}^{n} b_i\otimes y_i$，考虑到它们在 $\bigoplus_{y\in Y}A_y$ 中的象，可知 $a_i\otimes y_i=b_i\otimes y_i$ $(1\leqslant i\leqslant n)$. 于是由前所述，便有 $a_i=b_i(1\leqslant i\leqslant n)$. ▌

系 1 设 A 和 B 分别是以 X 和 Y 为基的自由 R-模，则 $A\otimes_R B$ 也是自由 R-模，并且 $\{x\otimes y\mid x\in X, y\in Y\}$ 是它的一组 R-基.

证明 A 中元素均可表为 $a=\sum_i r_i x_i$ (有限和，$r_i\in R$，$x_i\in X$)，B 中元素均可表为 $b=\sum_j s_j y_j$(有限和，$s_j\in R, y_j\in Y$)，从而 $a\otimes b=\sum_{i,j} r_i s_j x_i\otimes y_j$(有限和). 而 $A\otimes_R B$ 是由这种 $a\otimes b$ 生成的. 这就表明 $A\otimes_R B$ 中每个元素均是 $\{x\otimes y\mid x\in X, y\in Y\}$ 中元

素的 R-线性组合. 另一方面,如果$\sum_{i,j} r_{ij}x_i\otimes y_j=\sum_{i,j} r'_{ij}\, x_i\otimes y_j$(有限和,$r_{ij},r'_{ij}\in R$,诸 x_i 两两不同,诸 y_j 也两两不同),则由引理 10 可知,对每个 j 均有$\sum_i r_{ij}x_i=\sum_i r'_{ij}x_i$. 再由$X$是$R$-模$A$的基,即知对每组 i,j,均有 $r_{ij}=r'_{ij}$. 这样证明了表达式的唯一性.因此 $A\otimes_R B$ 为自由 R-模,并且$\{x\otimes y\mid x\in X,y\in Y\}$是$A\otimes_R B$的一组基. ▌

系 2 设R是S的子环,M是以X为基的自由R-模.则$S\otimes_R M$是以$\{1\otimes x\mid x\in X\}$为基的自由$S$-模.

证明 由引理 10 可知,将 $S\otimes_R M$ 看作是 R-模时,每个元素均可表为$\sum_{i=1}^{n} s_i\otimes x_i=\sum_{i=1}^{n} s_i(1\otimes x_i)$ ($s_i\in S,x_i\in X$,且诸 x_i 两两不同). 从而 $S\otimes_R M$ 中元素均可表成$\{1\otimes x\mid x\in X\}$的$S$-线性组合. 进而,若$\sum_{i=1}^{n} s_i(1\otimes x_i)=\sum_{i=1}^{n} s'_i(1\otimes x_i)$,则$\sum_{i=1}^{n} s_i\otimes x_i=\sum_{i=1}^{n} s'_i\otimes x_i$. 由于$X$是$R$-模$M$的基,于是由引理 10 即知 $s_i=s'_i$ ($1\leqslant i\leqslant n$).这就表明$\{1\otimes x\mid x\in X\}$是$S$-模 $S\otimes_R M$的一组基,而$S\otimes_R M$是自由S-模. ▌

习　　题

(以下题中记 $\mathbf{Z}_m=\mathbf{Z}/m\mathbf{Z}$)

1. 设A为 Abel 群,求证:

(1) $A\otimes\mathbf{Z}_m\cong A/mA$ ($m\geqslant1$);

(2) $\mathbf{Z}_m\otimes\mathbf{Z}_n\cong\mathbf{Z}_{(m,n)}$ ($n,m\geqslant1$).

2. 设A为扭 Abel 群(即每个元素均是有限阶的),则 $A\otimes\mathbf{Q}=0$,但是$\mathbf{Q}\otimes\mathbf{Q}\cong\mathbf{Q}$.

3. 设 A' 和 B' 分别为R-模A和B的R-子模,求证有R-模同构

$$\frac{A}{A'}\otimes_R\frac{B}{B'}\cong\frac{A\otimes_R B}{C},$$

其中C是$A\otimes_R B$中由$\{a'\otimes b, a\otimes b' \mid a\in A, a'\in A', b\in B, b'\in B'\}$生成的$R$-子模.

4．设$\alpha: Z_2\to Z_4$是Abel群的唯一的非零同态。求证 $1\otimes\alpha: Z_2\otimes Z_2\to Z_2\otimes Z_4$是零同态。

5．求证下列三个命题是彼此等价的：

(1) $0\to A\xrightarrow{f} B\xrightarrow{g} C\to 0$是分裂的$R$-模短正合序列。

(2) 对于每个R-模D, $0\to D\otimes_R A\xrightarrow{1\otimes f}D\otimes_R B\xrightarrow{1\otimes g}D\otimes_R C\to 0$均是分裂的$R$-模短正合序列。

(3) 对于每个R-模D，$0\to A\otimes_R D\xrightarrow{f\otimes 1}B\otimes_R D\xrightarrow{g\otimes 1}C\otimes_R D\to 0$均是分裂的$R$-模短正合序列。

6．设$\mathfrak{a}$为环R的理想，M为R-模。则有R-模同构

$$\frac{R}{\mathfrak{a}}\otimes_R M\cong\frac{M}{\mathfrak{a}M}$$

其中　$\mathfrak{a}M=\{$有限和$\sum a_i m_i \mid a_i\in\mathfrak{a},\ m_i\in M\}$为$M$的$R$-子模。

7．设$\mathfrak{a}$和$\mathfrak{b}$均是环R的理想，则有R-模同构

$$\frac{R}{\mathfrak{a}}\otimes_R\frac{R}{\mathfrak{b}}\cong\frac{R}{\mathfrak{a}+\mathfrak{b}}.$$

8.设R为局部环，M和N均是有限生成R-模，求证：$M\otimes_R N=0\Longleftrightarrow M=0$或者$N=0$. [提示：利用习题6,7,证明$\frac{M}{\mathfrak{m}M}\otimes_R\frac{N}{\mathfrak{m}N}\cong\frac{M\otimes_R N}{\mathfrak{m}(M\otimes_R N)}$,然后利用中山引理.]

9．求证多项式环$R[x]$为平坦R-模。

10．求证：N为平坦R-模的充要条件是：如果$M'\xrightarrow{f}M\xrightarrow{g}M''$为$R$-模正合序列，则$M'\otimes_R N\xrightarrow{f\otimes 1}M\otimes_R N\xrightarrow{g\otimes 1}M''\otimes_R N$也为$R$-模正合序列。[提示：正合序列$M'\xrightarrow{f}M\xrightarrow{g}M''$等价于如下两个正合序列：$0\to\mathrm{Ker} f\xrightarrow{i}M'\xrightarrow{f}\mathrm{Im} f\to 0$和$0\to\mathrm{Ker} g\xrightarrow{i}M\xrightarrow{g}\mathrm{Im} g\to 0$.]

11．设$f: A\to B$为环的同态，由f将B作成A-模．如果M为平坦A-

模，求证 $B\otimes_A M$为平坦B-模.

12．设M和N均为平坦R-模，则$M\otimes_R N$ 也为平坦R-模。

13．设 $\mathfrak{a}$ 为环R的理想并且 $\mathfrak{a}\subseteq r(R)$（$R$的大根），$M$为$R$-模，$N$为有限生成$R$-模. $u:M\to N$为R-模同态.如果诱导同态 $\bar{u}:M/\mathfrak{a}M\to N/\mathfrak{a}N$ 为满射，求证 u 也为满射.

14．设M是有限生成R-模，$f:M\to R^n$为R-模满同态. 求证 $\mathrm{Ker}f$ 是有限生成R-模.[提示：设 $e_1,\cdots,e_n$ 是R^n 的一组R-基，$f(u_i)=e_i$ $(1\leqslant i\leqslant n)$，证明 M是 $\mathrm{Ker}f$ 和子模$\sum_{i=1}^{n}Ru_i$ 的直和.]

15．设$f:A\to B$ 为环的同态，M为B-模，经过f将M看成是A-模（$a\cdot m=f(a)m$）.然后再把这个A-模M 扩充成B-模 $M_B=B\otimes_A M$，求证：标准B-模同态 $g:M\to M_B$，$y\mapsto 1\otimes y$ 是单同态，并且 $g(M)$ 是B-模M_B的直和成份.[提示：定义 $p:M_B\to M$，$b\otimes y\to by$，求证$M_B=\mathrm{Im}\,g\oplus\mathrm{Ker}\,p$.]

16.设M，N，P 均是R-模，如果R-模M与N同构，则R-模$M\otimes_R P$ 和 $N\otimes_R P$ 也同构.

§ 2.6 主理想整环上的有限生成模

环R上有限生成模的结构和分类问题，是模论或环论的中心问题之一. 对于一般的环R，这个问题是困难的. 当R为域时，这个问题是容易的 因为域R上有限生成模就是有限维R-向量空间，而两个有限维向量空间同构的充要条件是它们具有相同的维数. 本节我们解决R是主理想整环的情形，给出有限生成R-模的结构和分类定理. 特别取 $R=\mathbf{Z}$，我们就得到有限生成 Abel 群的结构和分类结果. 最后我们还谈一下本节结果在线性代数中的一个应用. 我们在第五章还要给出 Dedekind 整环上有限生成模的结构和分类的完整结果.

关于主理想整环上的有限生成模，其最关键的结果是

定理 12 设R是主理想整环，M为秩 n 的自由R-模，则

(A) M的每个R-子模 M'也是自由 R-模,并且 $\mathrm{rank}_R M' \leqslant n$.

(B) 存在 $e_1,\cdots,e_n\in M, a_1,\cdots,a_q\in R$, $a_1|a_2|\cdots|a_q$, $q\leqslant n$, 使得

$$M=Re_1\oplus\cdots\oplus Re_n, M'=Ra_1e_1\oplus\cdots\oplus Ra_qe_q.$$

注记 设a和b是整环R中的元素,则$a|b$(a整除b)是指有$c\in R$使得$b=ac$. 这也相当于说$(b)\subseteq(a)$.

证明 我们首先需要作些准备工作. 不妨设$M'\neq 0$, 对于每个$u\in \mathrm{Hom}_R(M,R)$, $u(M')$是R的子模,即为R的理想, 从而是主理想. 于是$u(M')=(a_u)$, $a_u\in R$. 考虑R的理想集合

$$\Sigma=\{(a_u)\mid u\in \mathrm{Hom}_R(M,R)\}.$$

取$u=0$可知零理想属于Σ,从而Σ是非空集合. 我们可以不用Zorn引理而用反证法直接证明Σ有极大元: 假如对于Σ中每个理想$\mathfrak{a}$,都有理想$\mathfrak{b}\in\Sigma$大于$\mathfrak{a}$,我们就得到无限递增理想升链$\mathfrak{a}_1\subset\mathfrak{a}_2\subset\cdots\subset\mathfrak{a}_n\subset\cdots$,易证$\mathfrak{a}=\bigcup\limits_{n=1}^{\infty}\mathfrak{a}_n$也是$R$中理想. 于是$\mathfrak{a}=(a)$. 由于$a\in\mathfrak{a}$,从而$a$必属于某个$\mathfrak{a}_n$. 于是$\mathfrak{a}_n\subset\mathfrak{a}_{n+1}\subseteq\mathfrak{a}=(a)\subseteq\mathfrak{a}_n$. 这就导致矛盾. 于是$\Sigma$包含极大元. 设$a_uR=(a_u)$是$\Sigma$中一个极大元, $u\in\mathrm{Hom}_R(M,R)$. 任取R-模M的一组基$x_1,\cdots,x_n$,即$M=\bigoplus\limits_{i=1}^{n}Rx_i$. 令

$$p_i: M\to R,\ p_i\left(\sum_{k=1}^{n}a_kx_k\right)=a_i,$$

则$p_i\in\mathrm{Hom}_R(M,R)$ $(1\leqslant i\leqslant n)$. 由于$M'\neq 0$,可知至少有一个$i$使得$p_i(M')\neq 0$. 但是$p_i(M')\in\Sigma$. 这就表明$\Sigma$中包含非零理想. 特别地,$\Sigma$中的极大元$(a_u)$不是零理想,即$a_u\neq 0$,于是$u\neq 0$ 令$e'\in M'$使$u(e')=a_u$,则$e'\neq 0$ 进而,对于每个$v\in\mathrm{Hom}_R(M,R)$,必然$a_u|v(e')$. 因为若令$d=(a_u,v(e'))$,则有$b,c\in R$,使得

$d=ba_u+cv(e')$. 于是 $d=(bu+cv)(e')=w(e')$,其中 $w=bu+cv\in \mathrm{Hom}_R(M,R)$. 从而$(a_u)\subseteq(d)\subseteq w(M')\in\Sigma$. 由$(a_u)$的极大性即知$(a_u)=(d)$. 但是 $d=(a_u,v(e'))$,从而必然 $a_u|v(e')$. 特别地我们有 $a_u|p_i(e')(1\leqslant i\leqslant n)$. 这表明 e' 表成$x_1,\cdots,x_n$的 R-线性组合式时 a_u 除尽全部系数. 从而有 $e\in M$ 使得 $e'=a_ue$. 于是 $a_u=u(e')=u(a_ue)=a_uu(e)$. 由于 $a_u\neq0$, 从而 $u(e)=1$.

现在我们要证明:

$$M=Re\oplus\mathrm{Ker}\,u, \tag{1}$$

$$M'=Re'\oplus(M'\cap\mathrm{Ker}\,u). \tag{2}$$

对于每个 $x\in M$, $x=u(x)e+(x-u(x)e)$,而 $u(x-u(x)e)=u(x)-u(x)u(e)=0$ (因为 $u(e)=1$). 这就表明 $x-u(x)e\in\mathrm{Ker}\,u$. 从而

$$M=Re+\mathrm{Ker}\,u. \tag{3}$$

类似地,对于 $y\in M'$,则$u(y)=ba_u,b\in R$(因为$u(y)\in u(M')=(a_u)$). 于是 $y=ba_ue+(y-u(y)e)=be'+(y-u(y)e)$,而 $y-u(y)e\in\mathrm{Ker}\,u$. 这就证明了

$$M'=Re'+(M'\cap\mathrm{Ker}\,u). \tag{4}$$

我们还需要证明(3)和(4)式右边均是直和. 这相当于要证明 $Re\cap\mathrm{Ker}\,u=0$, $Re'\cap(M'\cap\mathrm{Ker}\,u)=0$. 我们只需证明第一式,因为由第一式立得第二式. 设 $x\in Re\cap\mathrm{Ker}\,u$,则 $x=ce,c\in R$, 并且 $u(x)=0$. 于是 $0=u(x)=u(ce)=cu(e)=c$, 从而 $x=ce=0\cdot e=0$. 这就表明 $Re\cap\mathrm{Ker}\,u=0$. 于是我们证明了(1)和(2)式.

有了以上的准备, 我们现在来证明定理中的(A). 由于M中最多有 n 个元素是 R-线性无关的(§2.2 习题 4),从而它的子模也是如此. 所以我们只需对每个 $r(0\leqslant r\leqslant n)$ 归纳证明如下的命题即可.

命题 $P(r)$: 如果M的 R-子模N至多只有 r 个元素是 R-线

性无关的，则N是自由R-模.

$P(0)$显然正确. 设$q\geqslant 1$，而当$r<q$时$P(r)$均成立. 如果子模$M'\neq 0$，并且至多有q个元素是R-线性无关的. 对于M'按本证明前部分所述，我们就得到(2)式. 其中子模$M'\cap \mathrm{Ker}\,u$中R-线性无关元素显然不能超过$q-1$个. 从而由归纳假设可知$M'\cap\mathrm{Ker}\,u$为自由R-模. 于是$M'=Re'\oplus(M'\cap\mathrm{Ker}u)$也是自由$R$-模. 即$P(q)$成立. 这就证明了$(A)$.

再证定理中的(B). 我们对$n=\mathrm{rank}_R M$归纳. $n=0$时(B)显然成立. 假设M的秩小于n时(B)均成立. 我们根据(A)知道$\mathrm{Ker}\,u$为自由R-模. 而由(1)式可知$\mathrm{rank}_R(\mathrm{Ker}\,u)=n-1$. 对于$\mathrm{Ker}\,u$和它的子模$M'\cap\mathrm{Ker}\,u$利用归纳假设，可知有$e_2,\cdots,e_n\in\mathrm{Ker}u$，$a_2,\cdots,a_q\in R$，$a_2|a_3|\cdots|a_q$，$q\leqslant n$，使得

$$\mathrm{Ker}u=Re_2\oplus\cdots\oplus Re_n,$$

$$M'\cap\mathrm{Ker}u=Ra_2e_2\oplus\cdots\oplus Ra_qe_q.$$

于是令$a_1=a_u$，$e_1=e$，注意$e'=a_ue$，从而由(1)和(2)式得到

$$M=Re_1\oplus\cdots\oplus Re_n,\ M'=Ra_1e_1\oplus\cdots\oplus Ra_qe_q.$$

但是我们还需要证明$a_1|a_2$. 由于$e_1,\cdots,e_n$是R-模M的基，从而可定义$v\in\mathrm{Hom}_R(M,R)$，使得

$$v(e_1)=v(e_2)=1,v(e_3)=\cdots=v(e_n)=0.$$

于是$a_1=a_u=v(a_ue_1)=v(e')\in v(M')$. 因此$(a_u)\subseteq v(M')\in\Sigma$. 由于$(a_u)$为$\Sigma$中极大元，可知$v(M')=(a_u)=(a_1)$. 但是$a_2=v(a_2e_2)\in v(M')$，从而$a_2\in(a_1)$，即$a_1|a_2$. 这就完成了定理12的证明. ▌

注记 习题6是定理12的矩阵形式. 并且我们这里给出的证明实际上也就是通常将一个方阵化成在初等变换下与它等价的对角阵的方法. 不过我们这里不是在域上而是在主理想整环上作这件事情.

定理 12 是关于自由 R-模的结果．我们知道，如果 R 是整环，则自由 R-模都是无扭模．所以对于任意的有限生成 R-模，我们还要考虑它的扭子模 $T(M)$．下面的结果是令人愉快的．

引理 12 设 R 为主理想整环，M 为有限生成 R-模．

(1) 如果 M 为无扭模，则 M 必为自由 R-模．

(2) 在一般情形下，M 中存在秩有限的自由 R-子模 F，使得 $M=F\oplus T(M)$．

证明(1) 不妨设 $M\neq 0$．设 X 是 R-模 M 的一个有限的生成元集合．$S=\{x_1,\cdots,x_n\}$ 是 X 的一个极大 R-线性无关子集合．由于 $M\neq 0$，从而 X 中有非零元素．又由于 M 是无扭的，每个非零元素均形成 R-线性无关的一元集合．因此 S 非空，即 $n\geqslant 1$．由 S 生成的 M 的 R-子模 F 显然是以 S 为基的自由 R-模，即 $F=\bigoplus_{i=1}^{n} Rx_i$．对于每个 $y\in X$，由 S 的极大性可知 $\{y,x_1,\cdots,x_n\}$ 是 R-线性相关的．从而有不全为零的 $r_y,r_1,\cdots,r_n\in R$，使得

$$r_y y+r_1x_1+\cdots+r_nx_n=0.$$

于是 $r_y y=-(r_1x_1+\cdots+r_nx_n)\in F$．由于 $x_1,\cdots,x_n$ 是 R-线性无关的．可知必然 $r_y\neq 0$．现在令 $r=\prod_{y\in X} r_y$，则 $r\neq 0$(因为 R 为整环而 r_y 均不为 0)．从而对每个 $y\in X$，均有 $ry\in F$．因为 X 生成 M，从而 $rM\subseteq F$．但是由定理 12，自由 R-模 F 的子模 rM 也是自由 R-模．最后定义

$$f:M\to rM,\ f(m)=rm\quad (m\in M).$$

这是 R-模满同态．由于 M 中没有扭元素并且 $r\neq 0$，从而 $\operatorname{Ker} f=0$．即 f 为 R-模同构．于是 M 同构于 rM，从而是自由 R-模．

(2) 我们有 R-模短正合序列

$$0\to T(M)\xrightarrow{i} M\xrightarrow{p} M/T(M)\to 0$$

但是 $M/T(M)$ 是无扭 R-模．由(1)知 $M/T(M)$ 是自由 R-模．所以也是投射 R-模．于是上面的正合序列是分裂的（定理 8 的

(4)). 所以 $T(M)$是M的直和成分，即 $M=F\oplus T(M)$，于是 $F\cong M/T(M)$，从而F是自由 R-模. 而由M的有限生成性质可知F的秩有限. ▌

注记 (1) 在直和分解式 $M=T(M)\oplus F$ 中，F 不是唯一决定的. 但是若又有 $M=T(M)\oplus F'$，则 $F\cong M/T(M)\cong F'$. 于是自由 R-模 F 和 F' 有相同的秩. 因此 $\text{rank}_R F=\text{rank}_R M/T(M)$是由$M$所唯一决定的. 我们把 $\text{rank}_R M/T(M)$叫作是有限生成 R-模M的**自由秩**. 不难证明：M的自由秩等于M中 R-线性无关元素的最大个数(习题 1).

(2) 若 R-模M不是有限生成的，则引理 12 中的(1)不一定正确(习题 7).

现在证明我们的主要结果——主理想整环上有限生成模的结构和分类.

定理 13 设 R 为主理想整环，M为有限生成 R-模.

(I) 存在 $n\geqslant 0, r_1,\cdots,r_t\in R(t\geqslant 0)$，$r_i$ 均不为 0 和单位，$r_1|r_2|\cdots|r_t$，使得

$$M\cong R^n\oplus R/(r_1)\oplus\cdots\oplus R/(r_t)\quad (R\text{-模同构}).$$

并且 n 和理想$(r_1),\cdots,(r_t)$由M所唯一决定.

(II) 存在$n\geqslant 0$ 和 R 中素元 $p_1,\cdots,p_k$(不必不同)$(k\geqslant 0)$，以及正整数 $s_1,\cdots,s_k$，使得

$$M\cong R^n\oplus R/(p_1^{s_1})\oplus\cdots\oplus R/(p_k^{s_k})\quad (R\text{-模同构}).$$

并且 n 和 R 的理想$(p_1^{s_1}),\cdots,(p_k^{s_k})$由$M$所唯一决定.

注记 主理想整环 R 中的元素 p 叫作是**素元**，是指(p)为 R 的素理想.

证明 设 R-模M可以由m个元素生成，则M是秩为m的自由 R-模 F 的商模. 即存在 F 的子模 S，使得 $M\cong F/S$. 根据定理 12，S 为自由 R-模，并且存在F 的一组基 $e_1,\cdots,e_m$ 和非零元素

$a_1,\cdots,a_q\in R(q\leqslant m),a_1|a_2|\cdots|a_q$,使得

$$F=Re_1\oplus\cdots\oplus Re_m,S=Ra_1e_1\oplus\cdots\oplus Ra_qe_q.$$

于是

$$\begin{aligned}M\cong F/S&=(Re_1\oplus\cdots\oplus Re_m)/(Ra_1e_1\oplus\cdots\oplus Ra_qe_q)\\&\cong\frac{Re_1}{Ra_1e_1}\oplus\cdots\oplus\frac{Re_q}{Ra_qe_q}\oplus Re_{q+1}\oplus\cdots\oplus Re_m\\&\cong R/(a_1)\oplus\cdots\oplus R/(a_q)\oplus R^n\quad(n=m-q)\end{aligned}$$

设$a_1,\cdots,a_q$的前$q-t$个为R中单位,而后t个不为单位.并且记后t个为$r_1,\cdots,r_t$,则$r_1|r_2|\cdots|r_t$, $R/(a_i)\cong R/R=0(1\leqslant i\leqslant q-t)$从而

$$M\cong R^n\oplus R/(r_1)\oplus\cdots\oplus R/(r_t).$$

这就得到了(Ⅰ)中所述的表达式. 进而, 主理想整环R必然是唯一因子分解整环, 即R中每个不是单位的非零元素r均可唯一地表成$r\sim p_1^{\alpha_1}\cdots p_s^{\alpha_s}$其中$p_1,\cdots,p_s$是彼此互素的素元,$\alpha_i\geqslant 1(1\leqslant i\leqslant s)$,而$r\sim s$表示元素$r$和$s$相伴,即存在单位$u\in U(R)$使得$r=us$. (或者等价地说成:理想$(r)$和$(s)$相等.)由于理想$(p_1^{\alpha_1}),\cdots,(p_s^{\alpha_s})$是两两互素的,从而由中国剩余定理可知有$R$-模同构

$$R/(r)\cong R/(p_1^{\alpha_1})\oplus\cdots\oplus R/(p_s^{\alpha_s}).$$

将(I)的表达式中每个$R/(r_i)$都再作如此形式的分解, 我们就得到了(II)中的表达式.

现在谈(I)和(II)中表达式的唯一性问题. 我们从(II)中表达式开始. 不难看出n是R-模M的自由秩. 从而由M所决定. 于是$T(M)\cong R/(p_1^{s_1})\oplus\cdots\oplus R/(p_k^{s_k})$. 由于$p_1,\cdots,p_k$中可能有彼此相伴的素元,我们把$(p_1^{s_1}),\cdots,(p_k^{s_k})$重新排列成

$$\{(q_1^{\alpha_{11}}),\cdots,(q_1^{\alpha_{1t_1}}),(q_2^{\alpha_{21}}),\cdots,(q_2^{\alpha_{2t_2}}),\cdots,(q_\lambda^{\alpha_{\lambda 1}}),\cdots,(q_\lambda^{\alpha_{\lambda t_\lambda}})\},\tag{1}$$

其中$q_1,\cdots,q_\lambda$是彼此不相伴的素元,并且

$$1\leqslant\alpha_{11}\leqslant\cdots\leqslant\alpha_{1t_1},\cdots,1\leqslant\alpha_{\lambda_1}\leqslant\cdots\leqslant\alpha_{\lambda t_\lambda}\quad(t_1,\cdots,t_\lambda\geqslant 1).$$

$$(2)$$

于是 $T(M)\cong\bigoplus_{i=1}^{\lambda}T_i$，其中 $T_i=\bigoplus_{j=1}^{t_i}R/(q_i^{\alpha_{ij}})$. 如果 $\{\alpha_{i1},\cdots,\alpha_{it_i}\}$ 中有 s_l 个为 $l(1\leqslant l\leqslant N_i, N_i=\alpha_{it_i})$，则 $T_i=\bigoplus_{l=1}^{N_i}(R/(q_i^l))^{s_l}$.

我们已经知道：对于 R 的任意两个理想 $\mathfrak{a}$ 和 $\mathfrak{b}$，$R/\mathfrak{a}\otimes_R R/\mathfrak{b}\cong R/(\mathfrak{a}+\mathfrak{b})$（§2.5，习题 7）. 于是若 p 和 q 均为 R 中素元，$\alpha,\beta\geqslant 1$，则

$$R/(p^\alpha)\otimes_R R/(q^\beta)\cong R/((p^\alpha)+(q^\beta))$$
$$\cong\begin{cases}0, & \text{当}(p)\neq(q)\text{时},\\ R/(p^{\min(\alpha,\beta)}), & \text{当}(p)=(q)\text{时}.\end{cases}$$

从而对于 $1\leqslant\alpha\leqslant N_i$，

$$R/(q_i^\alpha)\otimes_R T(M)\cong R/(q_i^\alpha)\otimes_R\left(\bigoplus_{l=1}^{N_i}(R/(q_i^l))^{s_l}\right)$$

（§2.5，习题 16）

$$\cong\bigoplus_{l=1}^{N_i}(R/(q_i^\alpha)\otimes_R R/(q_i^l))^{s_l}$$

$$\cong\bigoplus_{l=1}^{\alpha-1}(R/(q_i^l))^{s_l}\oplus(R/(q_i^\alpha))^{s_\alpha+s_{\alpha+1}+\cdots+s_{N_i}}. \tag{3}$$

而当素元 q 与 $q_1,\cdots,q_\lambda$ 中任何一个均不相伴时，对每个 $\alpha\geqslant 1$ 均有

$$R/(q^\alpha)\otimes_R T(m)=0. \tag{4}$$

注意到，若 N 为 R-模，则对于 R 中每个主理想 (a)，$(a)N=\{ax\mid x\in N\}$ 也是 R-模. 并且若有 R-模同构 $N_1\cong N_2$，则 $(a)N_1\cong(a)N_2$. 又 $(a)(N_1\oplus N_2)=(a)N_1\oplus(a)N_2$. 于是由 (3) 式给出 R-模同构

$$(q_i^{\alpha-1})(R/(q_i^\alpha)\otimes_R T(M))\cong((q_i^{\alpha-1})/(q_i^\alpha))^{s_\alpha+\cdots+s_{N_i}}$$
$$\cong(R/(q_i))^{s_\alpha+\cdots+s_{N_i}}$$
$$(1\leqslant\alpha\leqslant N_i). \tag{5}$$

由(5)式可知等式右边可看成是$R/(q_i)$上的自由模，并且秩为$s_\alpha+\cdots+s_{N_i}$. 由于(3)，(4)和(5)式左边完全是R-模M的特性，从而由(3)和(4)式可知$(q_1),\cdots,(q_\lambda)$是由M所决定的. 对于每个i，$(1\leqslant i\leqslant\lambda)$，由(5)式可知$s_\alpha+\cdots+s_{N_i}(1\leqslant\alpha\leqslant N_i)$由$M$所决定，从而$s_\alpha(1\leqslant\alpha\leqslant N_i)$由$M$所决定. 因此$\{\alpha_{i1},\alpha_{i2},\cdots,\alpha_{it_i}\}$由$M$所决定. 这就表明集合(1)由$M$所决定，也就是$(p_1^{s_1}),\cdots,(p_k^{s_k})$由$M$所决定.

由(II)中表达式的唯一性不难推出(I)中表达式的唯一性. 因为集合(1)是将$r_1,\cdots,r_t$分解成“素元幂”的乘积之后，其全部“素元幂”所组成的集合. 由条件$r_1|r_2|\cdots|r_t$不难得到

$$(r_t)=(q_1^{\alpha_{1t_1}}\cdots q_\lambda^{\alpha_{\lambda t_\lambda}})$$

$$(r_{t-1})=\Big(\prod_{\substack{i=1\\t_i\geqslant 2}}^{\lambda} q_i^{\alpha_{i,t_i-1}}\Big)$$

$$\vdots$$

$$(r_l)=\Big(\prod_{\substack{i=1\\t_i\geqslant t-l+1}}^{\lambda} q_i^{\alpha_{i,t_i-l}}\Big)$$

$$\vdots$$

由于集合(1)由M所决定，从而由上面诸式可知$(r_1),\cdots,(r_t)$也由M所决定. 这就完全证明了定理 13. ▌

定义 定理 13 中的理想集合$\{(r_1),\cdots,(r_t)\}$叫作是有限生成R-模M的**不变因子**. 而$\{(p_1^{s_1}),\cdots,(p_k^{s_k})\}$叫作是$M$的**初等因子**.

由定理 13 立刻推出

系(主理想整环上有限生成模的分类) 设R是主理想整环，M和N均是有限生成R-模. 则下面三条件彼此等价：

(1) $M\cong N$(R-模同构)；

(2) M和N有相同的自由秩和不变因子；

(3) M和N有相同的自由秩和初等因子. ▌

现在我们给出定理 13 和它的系的两个应用. 第一个应用是取 $R=\mathbf{Z}$,立刻得到有限生成 Abel 群的结构和分类结果：

定理 14 (有限生成 Abel 群基本定理) 设A是有限生成 Abel 群,则

(I) $A\cong\mathbf{Z}^n\oplus\mathbf{Z}/n_1\mathbf{Z}\oplus\cdots\oplus\mathbf{Z}/n_t\mathbf{Z}$.

其中 $n\geqslant 0, t\geqslant 0$, $n_1\cdots$, $n_t\geqslant 2$, 并且 $n_1|n_2|\cdots|n_t$. 此外, n 和 $n_1,\cdots,n_t$ 是由群A所唯一决定的. (n 是A中 $\mathbf{Z}$-线性无关元素的最大个数,叫作是A的自由秩, 而$\{n_1,\cdots,n_t\}$ 叫作是A的不变因子.)

(II) $A\cong\mathbf{Z}^n\oplus\mathbf{Z}/p_1^{\alpha_1}\mathbf{Z}\oplus\cdots\oplus\mathbf{Z}/p_k^{\alpha_k}\mathbf{Z}$.

其中 $n\geqslant 0, p_1,\cdots,p_k$ 为素数(不必不同), $k\geqslant 0$. $\alpha_1,\cdots,\alpha_k\geqslant 1$. 此外$n$ 和$\{p_1^{\alpha_1},\cdots,p_k^{\alpha_k}\}$ 是由A所唯一决定的. ($\{p_1^{\alpha_1},\cdots,p_k^{\alpha_k}\}$ 叫作是A的初等因子.) ▌

系 设A和B是两个有限生成 Abel 群, 则下列三条件彼此等价.

(1) $A\cong B$(Abel 群同构)；

(2) A和B有相同的自由秩和不变因子；

(3) A和B有相同的自由秩和初等因子. ▌

第二个应用是域F上有限维空间V中线性变换(自同态)的标准形问题(用矩阵语言,则是域F上n阶方阵的相似标准形问题). 我们不想讲线性代数方面过多的细节, 而主要想表明采用模来处理这一问题是多么地自然和方便.

设V是域F上的n维向量空间. 固定V的一组基X之后, V

上每个F-线性变换 $\varphi\in\mathrm{Hom}_F(V,V)$对于固定基$X$可表示成$F$上的一个$n$阶方阵$A$,$\varphi$和$A$是一一对应的．并且若$\varphi$和$\psi$对于同一组基$X$分别对应于方阵$A$和$B$,则$\varphi\pm\psi$,$a\varphi(a\in F)$和$\varphi\psi$分别对应于方阵$A\pm B$,$aA$和$AB$．从而我们有

$\mathrm{Hom}_F(V,V)\cong\mathrm{Mat}_n(F)$（右边表示$F$上$n$阶方阵全体）．这既是环同构,也是$F$-模(即$F$-向量空间)同构．并且它们均是$n$维的$F$-向量空间．

对于$\varphi\in\mathrm{Hom}_F(V,V)$和多项式$f(x)=\sum\limits_{i=0}^{m}a_ix^i\in F[x]$，则

$f(\varphi)=\sum\limits_{i=0}^{m}a_i\varphi^i\in\mathrm{Hom}_F(V,V)$．（规定$\varphi^0=1_V$.）于是我们有映射

$$\zeta_\varphi:F[x]\to\mathrm{Hom}_F(V,V),f(x)\mapsto f(\varphi).$$

这是环的同态,也是F-模同态．由于$\dim_F F[x]=+\infty$,而$\dim_F\mathrm{Hom}_F(V,V)=n^2<+\infty$,从而$\mathrm{Ker}\zeta_\varphi\neq 0$．由于$F[x]$是主理想整环，从而$\mathrm{Ker}\zeta_\varphi$是$F[x]$的非零主理想．于是$\mathrm{Ker}\zeta_\varphi=(q_\varphi(x))$．其中$0\neq q_\varphi(x)\in F[x]$,并且如果取$q_\varphi(x)$为首一(即最高次项系数为1的)多项式,则$q_\varphi(x)$是由$\mathrm{Ker}\zeta_\varphi$从而由$\varphi$所唯一决定的．我们称$q_\varphi(x)$为**线性变换$\varphi$的极小多项式**．由这个定义可知$q_\varphi(x)$由以下两个性质所完全刻画：

(1) $q_\varphi(x)$为$F[x]$中首一多项式并且$q_\varphi(\varphi)=0$.

(2) 若$f(x)\in F[x]$,$f(\varphi)=0$,则$q_\varphi(x)\mid f(x)$.

类似地,对于每个方阵$A\in\mathrm{Mat}_n(F)$,定义

$$\zeta_A:F[x]\to\mathrm{Mat}_n(F),f(x)\mapsto f(A).$$

则有唯一的首一多项式$q_A(x)\in F[x]$,使得$\mathrm{Ker}\,\zeta_A=(q_A(x))$．我们称$q_A(x)$为**方阵A的极小多项式**．它也由以下两个性质所完全刻画：

(1′) $q_A(x)$为$F[x]$中首一多项式并且$q_A(A)=0$.

(2′) 若 $f(x)\in F[x]$并且 $f(A)=0$,则 $q_A(x)\mid f(x)$.
进而,如果 A 是 φ 对于 V 的某一组基之下的表示方阵,则 $q_\varphi(x)=q_A(x)$.

对于固定的 $\varphi\in \mathrm{Hom}_F(V,V)$,我们定义 $F[x]$ 在 V 上的作用为:

$$f(x)\cdot v=f(\varphi)\cdot v \quad (f(x)\in F[x], v\in V).$$

由此将 V 作成为 $F[x]$-模. 我们称 V 的这个模结构为 **φ-结构**. 于是, U 为 V 的 $F[x]$-子模恰好相当于说 U 是 V 的一个 φ-不变子空间.

例 对于每个向量 $v\in V$, $V(\varphi,v)=F[x]\cdot v=\{f(x)\cdot v\mid f(x)\in F[x]\}$是一个 φ-不变子空间. 我们将这类 φ-不变子空间叫作是 **φ-循环子空间**, 因为它是 V 中由 v 所生成的 $F[x]$-循环子模.

定理 15 设 $\varphi\in \mathrm{Hom}_F(V,V)$, 则

(I) 存在正次数首一多项式 $q_1(x),\cdots,q_t(x)\in F[x]$和 V 的 φ-循环子空间 $V_1,\cdots,V_t$. 使得

$$V=V_1\oplus\cdots\oplus V_t,\quad q_1(x)\mid q_2(x)\mid\cdots\mid q_t(x),$$

并且 $q_i(x)$是线性变换 $\varphi|_{V_i}:V_i\to V_i$ 的极小多项式. 进而, $q_1(x),\cdots,q_t(x)$由 φ 所唯一决定(叫作是 **φ 的不变因子**),并且 $q_\varphi(x)=q_t(x)$.

(II) 存在不可约首一多项式 $p_1(x),\cdots, p_s(x)\in F[x]$ (两两不同), V 中的 φ-循环子空间 $V_{11},\cdots,V_{1t_1},\cdots,V_{s1},\cdots,V_{st_s}$, 以及 $m_{i1}\geqslant m_{i2}\geqslant\cdots\geqslant m_{it_i}\geqslant 1(1\leqslant i\leqslant s)$. 使得

$$V=\bigoplus_{i=1}^{s}\bigoplus_{j=1}^{t_i}V_{ij},$$

并且 $p_i(x)^{m_{ij}}$ 为 $\varphi|_{V_{ij}}:V_{ij}\to V_{ij}$ 的极小多项式. 进而, 集合 $\{p_i(x)^{m_{ij}}\mid 1\leqslant i\leqslant s,\ 1\leqslant j\leqslant t_i\}$ 由 φ 所唯一决定 (叫作是 **φ 的初**

等因子)，并且 $q_\varphi(x)=p_1(x)^{m_{11}}\cdots p_s(x)^{m_{s1}}$.

证明 (I) 将 V 作成具有 φ-结构的 $F[x]$-模. 由于 V 作为 F-模是有限生成的，从而作为 $F[x]$-模也是有限生成的. 并且由于 $q_\varphi(\varphi)=0$，可知 $q_\varphi(x)\cdot V=q_\varphi(\varphi)V=0$. 这表明 V 是扭 $F[x]$-模，即作为 $F[x]$-模的自由秩是 0. 于是在定理 13 中取 R 为主理想整环 $F[x]$，可知有 $F[x]$-模直和分解：

$$V=V_1\oplus\cdots\oplus V_t,\quad V_i\cong F[x]/(q_i(x)),\ 1\leqslant i\leqslant t,$$
$$q_1(x)|q_2(x)|\cdots|q_t(x).$$

如果取 $q_i(x)$ 均为首一多项式，则它们由具有 φ-结构的 $F[x]$-模 V 所唯一决定，从而由 φ 所唯一决定. 由于 $F[x]/(q_i(x))$ 是由 $\bar{x}$ 生成的循环 $F[x]$-模，从而 $V_i(1\leqslant i\leqslant t)$ 也是循环 $F[x]$-模，即均为 φ-循环子空间. 并且 $\mathrm{Ann}(V_i)=\mathrm{Ann}(F[x]/(q_i(x))=(q_i(x))$. 所以 $q_i(x)$ 是 $\varphi|_{V_i}$ 的极小多项式. 最后

$$(q_\varphi(x))=\mathrm{Ann}(V)=\bigcap_{i=1}^{t}\mathrm{Ann}(V_i)=\bigcap_{i=1}^{t}(q_i(x))=(q_t(x)).$$

由于 $q_\varphi(x)$ 和 $q_t(x)$ 均是首一多项式，所以 $q_\varphi(x)=q_t(x)$.

(II) 由定理 13 中的(II)完全类似地得出. ▌

我们知道，对于线性变换 φ，如果向量空间 V 按定理 13 所述两种方式分解成一些 φ-不变子空间的直和，那末适当给出 V 的一组基使得 φ 对于这组基的表示方阵有分块方阵的形式. 现在我们再进一步给出每个方块的相似标准形.

引理13 (有理标准形) 设 $\varphi\in\mathrm{Hom}_F(V,V)$，则下面两条件是等价的.

(1) V 为 φ-循环子空间，并且 $q_\varphi(x)=x^r+a_1x^{r-1}+\cdots+a_r\in F[x]$；

(2) $\dim_F V=r$，并且 φ 对于 V 的某组基的表示方阵为

$$A=\begin{pmatrix} 0 & 1 & & & \\ & 0 & 1 & & \\ & & \ddots & \ddots & \\ & & & 0 & 1 \\ -a_r & -a_{r-1} & \cdots & & -a_1 \end{pmatrix}.$$

证明 (1)⇒(2)：令 $V=F[x]\cdot v$. 由于 $q_\varphi(x)$ 为 φ 的极小多项式，于是 $(q_\varphi(x))=\mathrm{Ann}(V)=\mathrm{Ann}(v)$. 从而对于每个 $0\neq f(x)\in F[x]$，如果 $\deg f(x)<r=\deg q_\varphi(x)$，必然 $f(x)\cdot v\neq 0$. 这就表明 $v,\varphi(v),\cdots,\varphi^{r-1}(v)$ 是 F-线性无关的. 另一方面，对于每个 $f(x)\in F[x]$，我们熟知有 $q(x),r(x)\in F[x]$，$\deg r(x)<r$，使得 $f(x)=q(x)q_\varphi(x)+r(x)$. 从而 $f(x)\cdot v=f(\varphi)\ v=(q_\varphi(\varphi)q(\varphi)+r(\varphi))\cdot v=r(\varphi)\cdot v$. 因此 $V=F[x]\cdot v$ 中每个元素均是 $v,\varphi(v),\cdots,\varphi^{r-1}(v)$ 的 F-线性组合. 这就表明 $v,\varphi(v),\cdots,\varphi^{r-1}(v)$ 是 V 的一组 F-基. 于是 $\dim_F V=r$. 容易验证

$$\varphi\begin{pmatrix} v \\ \varphi(v) \\ \vdots \\ \varphi^{r-1}(v) \end{pmatrix}=\begin{pmatrix} \varphi(v) \\ \varphi^2(v) \\ \vdots \\ \varphi^{r-1}(v) \\ (-a_r-a_{r-1}\varphi-\cdots-a_1\varphi^{r-1})(v) \end{pmatrix}$$

$$=A\begin{pmatrix} v \\ \varphi(v) \\ \vdots \\ \varphi^{r-1}(v) \end{pmatrix}.$$

即 A 为 φ 对于基 $\{v,\varphi(v),\cdots,\varphi^{r-1}(v)\}$ 的表示方阵.

(2)⇒(1)：假设 A 为 φ 对于 V 的某组基 $\{v=v_1,v_2,\cdots,v_r\}$ 的表示方阵. 由 A 的形式可知

$$\left.\begin{aligned} &v_2=\varphi(v_1)=\varphi(v),\cdots,v_r=\varphi^{r-1}(v), \\ &\varphi^r(v)=\varphi(v_r)=-a_rv-a_{r-1}\varphi(v)-\cdots-a_1\varphi^{r-1}(v). \end{aligned}\right\}\ (*)$$

于是V是由v生成的φ-循环子空间. 即$F[x]\cdot v=V$. 由(*)中最后一式可知对于$q(x)=x^r+a_1x^{r-1}+\cdots+a_{r-1}x+a_r$有$q(\varphi)(v)=0$. 从而$q(\varphi)V=0$. 但是$\{v,\varphi(v),\cdots,\varphi^{r-1}(v)\}=\{v_1,v_2,\cdots,v_r\}$是$F$-线性无关的. 因此当$0\neq f(x)\in F[x]$, $\deg f(x)<r$时, 必然$f(x)\cdot v\neq 0$. 这就表明$q(x)$为φ的极小多项式. ▌

引理 14(Jordan 标准形) 设$\psi\in \mathrm{Hom}(V,V)$, 则下列两条件是等价的:

(1) V为ψ-循环子空间, 且$q_\psi(x)=(x-b)^r$, $b\in F$, $r\geqslant 1$;

(2) $\dim_F(V)=r$, 并且ψ对于V的某组基的表示方阵为

$$A=\begin{pmatrix} b & 1 & & & \\ & b & 1 & & \\ & & \ddots & \ddots & \\ & & & & 1 \\ & & & & b \end{pmatrix}.$$

证明 令$\varphi=\psi-b\cdot 1_V\in \mathrm{Hom}_F(V,V)$. 我们有两种方式将$V$作成$F[x]$-模. 一种是$\varphi$-结构: $f(x)\odot_\varphi v=f(\varphi)v$, 另一种是$\psi$-结构: $f(x)\odot_\psi v=f(\psi)v \quad (v\in V)$. 于是:

$$f(x)\odot_\varphi v=f(\varphi)v=f(\psi-b\cdot 1_V)v=f(x-b)\odot_\psi v \quad (v\in V).$$

由于映射

$$F[x]\to F[x],\ f(x)\mapsto f(x-b)$$

是一一对应. 不难看出:

(i) $(x-b)^r$为ψ的极小多项式$\Longleftrightarrow x^r$为φ的极小多项式;

(ii) V为ψ-循环子空间$\Longleftrightarrow V$为φ-循环子空间.

于是引理中条件(1)等价于:"V是φ-循环子空间并且φ的极小多项式为x^r". 根据引理13, 这又等价于"$\dim_F V=r$, 并且φ对于V的某组基X的表示方阵为$\begin{pmatrix} 0 & 1 & & \\ & 0 & 1 & \\ & & \ddots & \ddots \\ & & & 1 \\ & & & 0 \end{pmatrix}$". 由于$\psi=\varphi+b\cdot 1_V$.

从而这后一条件等价于引理中的条件(2)，因为$\psi=\varphi+b\cdot 1_V$对于基X的表示方阵为

$$\begin{pmatrix} 0 & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & 0 \end{pmatrix}+\begin{pmatrix} b & & \\ & \ddots & \\ & & b \end{pmatrix}=\begin{pmatrix} b & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & b \end{pmatrix}. \blacksquare$$

这样一来，我们就得到域F上n阶方阵的相似标准形的一般形式(先分块，然后每个块阵再化成有理标准形或Jordan标准形)．还应当指出的是：我们是在任意域F上进行的．对于每个特定的(或特定类型的)域，比如有理数域Q，代数封闭域(例如复数域)或者有限域，根据在这些域上多项式因子分解的不同特点，还可给出更具体的结果．

习　题

1．设R为主理想整环，M为有限生成R-模．求证M的自由秩等于M中R-线性无关元素的最大个数．

2．设R为主理想整环，K为R的商域．M为自由秩是r的有限生成R-模．求证有K-向量空间同构$K\otimes_R M\cong K^r$．

3．试问共有多少彼此不同构的360阶Abel群?

4．设R为主理想整环，$r,s\in R$，且r和s均不为0和单位，而且r和s也不互素．求证R-模$R/(r)\oplus R/(s)$的不变因子为$(r,s)R$和$[r,s]R$，其中(r,s)和$[r,s]$分别表示r和s的最大公因子和最小公倍元．

5．设R为(具有幺元素的交换)环．则R为主理想整环$\Longleftrightarrow$对于每个秩有限的自由R-模M，M的子模均是自由模．[提示：$\Leftarrow$：证明R的每个非零理想$\mathfrak{a}$均为自由R-模，然后证R-模$\mathfrak{a}$的基只能是一个元素．最后证环R没有不为0的零因子．]

6．(定理12的矩阵形式) 设R为主理想整环．A是R上的n阶方阵(即$A\in\mathrm{Mat}_n(R)$)，求证存在$B,C\in\mathrm{Mat}_n(R)$，$\det B,\det C\in U(R)$，使得

$$BAC=\begin{pmatrix} a_1 & & & & & & \\ & a_2 & & & & & \\ & & \ddots & & & & \\ & & & a_q & & & \\ & & & & 0 & & \\ & & & & & \ddots & \\ & & & & & & 0 \end{pmatrix}$$

其中 $0\neq a_i\in R(1\leqslant i\leqslant q)$，$a_1|a_2|\cdots|a_q$。并且满足这些条件的 $a_1,\cdots,a_q$ 由 A 所唯一决定。

7．证明 **Q** 是无扭 **Z**-模(无扭 Abel 群)，但不是自由 **Z**-模(自由 Abel 群)。

8．设 A 为有限 Abel 群，$\mathbf{C}^*$ 为非零复数乘法(Abel)群。求证：

(1) $A\cong\mathrm{Hom}(A,\mathbf{C}^*)$ (Abel 群同构)。

(2) 对于 A 的每个商群 B，均存在 A 的某个子群同构于 B。［提示：设 $B=A/C$，将 $\mathrm{Hom}(\ \ ,\mathbf{C}^*)$ 作用于 Abel 群短正合序列 $0\to C\to A\to A/C\to 0$，然后利用(1)。］

(3) 对于 A 的每个子群 B，均存在 A 的某个商群同构于 B。

9．设 M 为主理想整环 R 上的有限生成模，则 M 的每个子 R-模仍是有限生成 R-模。

10．设 R 为主理想整环，N_1,N,N_2 是有限生成 R-模。$0\to N_1\to N\to N_2\to 0$ 为 R-模正合序列。求证 N 的自由秩等于 N_1 和 N_2 的自由秩之和。

11．设 A 是由 a,b,c,d 生成的 Abel 群，定义关系为：$3b+2c+8d=0$，$5a+b-4c+8d=0$，$-2a+b+4c-8d=0$，$-a+3b+2c+8d=0$。试将 A 表成循环群的直和。并求 A 的自由秩，初等因子和不变因子。

12．设 A 是由 a,b,c 生成的自由 Abel 群，B 是由 $3a+9b+9c$ 和 $9a-3b+9c$ 生成的 A 的子群。求 A/B 的自由秩，初等因子和不变因子。

第三章　分式环和分式模，局部化方法

分式环和分式模以及与之相关联的局部化方法是交换代数中一个重要工具，它来源于直观的几何背景．例如在代数几何中，我们需要研究一个代数簇在某点或某点附近的局部性质，并且希望从各点的局部特性来把握代数簇的整体特性，这种方法在代数数论中也得到很成功的应用．通过德国数学家 Hasse 等人的工作，在数论研究中明确地给出由局部把握整体的一般思想原则，在二次型等许多方面解决了不少数论问题．现在，局部化方法已成为整个代数学(以及分析和几何学)中一个有效的一般方法．因此，本章篇幅虽然不长，但是我们在本章中介绍的关于分式环和分式模概念以及局部化方法，将在以后几章中不断地使用．

§ 3.1　分　式　环

我们在近世代数课中学过由整环 R 构作它的商域 K．办法是：令 $R^*=R-\{0\}$，在集合 $R\times R^*$ 中定义如下的二元关系：设 $(a,b),(c,d)\in R\times R^*$，$(a,b)\sim(c,d)\Longleftrightarrow ad=bc$．这是一个等价关系．由此把 $R\times R^*$ 分成一些等价类．我们把 (a,b) 所在的等价类表示成 a/b．以 K 表示全部等价类组成的集合．在 K 上自然地定义加法和乘法：

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd},\qquad \frac{a}{b}\cdot\frac{c}{d}=\frac{ac}{bd}.$$

则 K 由此成为域．并且通过环的单同态 $R\to K$，$a\mapsto\frac{a}{1}$ 可将 R 看成是 K 的子环．称 K 为 R 的商域，K 是包含 R 的最小域．

由 R 扩充成 K 的最大好处自然是：R 的每个非零元素在 K 中均可作为分母，即可除 R 中每个元素．由于域比环处理方便，所以环 R 中的数学问题放到域 K 上去考虑，可使我们增大视野和工作

的自由程度.

现在我们将这种思想加以推广. 首先我们不限定R为整环，而只假定R为任意带有幺元素的交换环. 其次我们不再要求R中每个非零元素均可作为分母,而是希望R中某个子集合S中的元素能够作分母. 而S的选取方式可以很多，因为我们只要求S满足下面定义中给出的不算苛刻的条件.

定义 设R为环. R的子集合S叫作是R的一个**乘法集**，是指它满足如下两个条件：

(1) $1\in S$；

(2) 若$a,b\in S$,则$ab\in S$.

设S为R的乘法集. 我们在集合$R\times S$上定义如下的二元关系：对于$(a,s),(b,t)\in R\times S$,

$(a,s)\sim(b,t)\Longleftrightarrow$存在$u\in S$,使得$u(at-bs)=0$.

这是一个等价关系. 因为自反性和对称性是容易验证的. 而传递性是由于：$(a,s)\sim(b,t),(b,t)\sim(c,u)\Rightarrow$有$v,w\in S$,使得$v(at-bs)=w(bu-ct)=0\Rightarrow tvw(au-cs)=0$(注意由$t,v,w\in S$可知$tvw\in S$)$\Rightarrow(a,s)\sim(c,u)$.

以a/s表示$(a,s)\in R\times S$所在的等价类. 以$S^{-1}R$表示$R\times S$的全部等价类组成的集合. 我们在$S^{-1}R$上如下定义加法和乘法：

$$\frac{a}{s}+\frac{b}{t}=\frac{at+bs}{st},\qquad \frac{a}{s}\cdot\frac{b}{t}=\frac{ab}{st}$$

(注意由$s,t\in S$可知$st\in S$).

当然要证明如此定义的运算与等价类a/s和b/t中代表元的选取无关. 以加法为例,就是要证明：若$a/s=a_1/s_1$, $b/t=b_1/t_1$,则$\dfrac{at+bs}{st}=\dfrac{a_1t_1+b_1s_1}{s_1t_1}$. 这是因为：

$$\left.\begin{array}{l}a/s=a_1/s_1\Rightarrow \text{有 } u\in S \text{ 使得 } u(as_1-a_1s)=0\\ b/t=b_1/t_1\Rightarrow \text{有 } v\in S \text{ 使得 } v(bt_1-b_1t)=0\end{array}\right\}\Rightarrow$$

$$\Rightarrow uv[(at+bs)s_1t_1-(a_1t_1+b_1s_1)st]=(as_1-a_1s)u\cdot tt_1v+(bt_1-b_1t)v\cdot ss_1u=0$$

$$\Rightarrow \frac{at+bs}{st}=\frac{a_1t_1+b_1s_1}{s_1t_1}.$$

对于乘法也可类似证明.

不难验证,$S^{-1}R$ 对于如此定义的加法和乘法是具有幺元素 1/1 的交换环. 零元素为 0/1(注意 $1\in S$). 我们称 $S^{-1}R$ 是**环 R 对于乘法集 S 的分式环.**

映射 $$f: R\to S^{-1}R, a\mapsto a/1 \quad (a\in R)$$
是环的同态. 但通常这不是单同态,即 Ker f 不一定为 0. 从而一般我们不能把 R 看成是 $S^{-1}R$ 的子环. 事实上,我们可以对 Ker f 作如下的刻画:

引理 1 $\operatorname{Ker}f=\{a\in R\mid \text{存在 } s\in S \text{ 使得 } sa=0\}$.

证明 如果 $a\in\operatorname{Ker}f$, 则$\frac{a}{1}=\frac{0}{1}$. 从而有 $s\in S$ 使得 $s(a\cdot 1-0\cdot 1)=0$,即 $sa=0$. 反之,若 $a\in R$,并且有 $s\in S$ 使得 $sa=0$,则在 $S^{-1}R$ 中(注意这时 s 可作分母),

$$f(a)=\frac{a}{1}=\frac{a}{1}\cdot\frac{s}{s}=\frac{as}{s}=\frac{0}{s}=\frac{0}{1}.$$

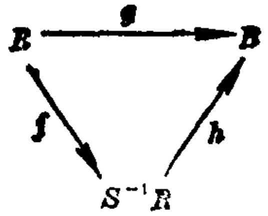
于是 $a\in\operatorname{Ker}f$. ▍

由引理 1 直接得出

系 $f: R\to S^{-1}R, a\mapsto a/1$ 是环的单同态(从而 R 可看成是 $S^{-1}R$ 的子环)$\Longleftrightarrow S$ 中没有元素是 R 的零因子. ▍

环 $S^{-1}R$ 有如下形式的泛性质:

引理 2 设 $g: R\to B$ 是环的同态, S 为 R 的乘法集, 并且 $g(S)\subseteq U(B)$(B 的单位群). 则有唯一的环同态 $h: S^{-1}R\to B$,使得(环和环同态)图表



是交换的(这里 $f: R\to S^{-1}R$ 为 $a\mapsto a/1$)。

证明 (1)存在性：定义 $h: S^{-1}R\to B, h(a/s)=g(a)g(s)^{-1}$ (注意 $s\in S\Rightarrow g(s)\in U(B)$)。这里需要验证 h 的可定义性，即若$\frac{a}{s}=\frac{a'}{s'}\in S^{-1}R$，则 $g(a)g(s)^{-1}=g(a')g(s')^{-1}$。这是因为：

$$\begin{aligned}\frac{a}{s}=\frac{a'}{s'}&\Rightarrow \text{有 } u\in S \text{ 使得 } u(as'-a's)=0\\ &\Rightarrow g(u)(g(a)g(s')-g(a')g(s))=0\\ &\Rightarrow g(a)g(s')=g(a')g(s) \qquad (\text{因为 } g(u)\in U(B))\\ &\Rightarrow g(a)g(s)^{-1}=g(a')g(s')^{-1}\\ &\qquad (\text{因为 } g(s),g(s')\in U(B)).\end{aligned}$$

易知 h 为环的同态，并且对每个 $a\in R$，

$$hf(a)=h(a/1)=g(a)g(1)^{-1}=g(a).$$

从而 $hf=g$。

(2) 唯一性：设 $h: S^{-1}R\to B$ 为环的同态，并且 $g=hf$。则对于每个 $a\in R$ 均有 $h(a/1)=hf(a)=g(a)$。从而对每个 $s\in S$ 均有 $h(1/s)=h((s/1)^{-1})=h(s/1)^{-1}=g(s)^{-1}$。于是对每个 $a/s\in S^{-1}R$，均有 $h(a/s)=h\left(\frac{a}{1}\cdot\frac{1}{s}\right)=h\left(\frac{a}{1}\right)h\left(\frac{1}{s}\right)=g(a)g(s)^{-1}$。这就证明了 h 的唯一性。▌

现在我们举一些分式环的例子。

例 1 如果 S 为环 R 的乘法集，并且 $0\in S$。不难看出 $S^{-1}R=0$(习题 1)。通常我们对此种情形不感兴趣。

例 2 如果 R 为整环，则 $S=R^*=R-\{0\}$ 是 R 的乘法集。并

且 $S^{-1}R$ 就是 R 的商域. 而且对于任意乘法集 S_1, $S_1^{-1}R$ 都可看成是 R 之商域的子环.

例 3 若 R 为环, $0\neq f\in R$. 则 $S=\{f^n|n\geqslant 0\}$ 显然是 R 的乘法集. 这时, $S^{-1}R$ 包含 R 为子环的充要条件是 f 不为 R 的零因子. 比如对于 $R=\mathbf{Z}$, n 为一个任意的正整数. 则对于 $S=\{n^r|r\geqslant 0\}$, $S^{-1}R=\bigcup_{r\geqslant 0}n^{-r}\mathbf{Z}$, 即为以 n 的方幂为分母的有理数所组成的环.

例 4 最重要的情形是 $S=R-\mathfrak{p}$, 其中 $\mathfrak{p}$ 是环 R 的素理想. S 为乘法集(由 $\mathfrak{p}\neq R$ 可知 $1\notin\mathfrak{p}$, 从而 $1\in S$; 由 $a,b\in S$ 可知 $a\notin\mathfrak{p}$, $b\notin\mathfrak{p}$ 从而 $ab\notin\mathfrak{p}$, 即 $ab\in S$). 对于 $S=R-\mathfrak{p}$ 这种情形, 我们把分式环 $S^{-1}R$ 通常写成 $R_\mathfrak{p}$, 叫作是**环 R 在 $\mathfrak{p}$ 处的局部化**. 比如对于 $R=\mathbf{Z}$, $\mathfrak{p}=(p)$ (p 为素数), 则不难看出

$$\mathbf{Z}_{(p)}=\left\{\frac{a}{b}\,\middle|\,a,b\in\mathbf{Z},(p,b)=1\right\}.$$

换句话说, 在 $\mathbf{Z}_{(p)}$ 中, 每个与 p 互素的整数均可作为分母. 这已经相当接近于 $\mathbf{Z}$ 的商域——有理数域 $\mathbf{Q}$ 了. 我们可以期望环 $\mathbf{Z}_{(p)}$, 或者更一般地, 局部化 $R_\mathfrak{p}$ 有比较简单的结构.

引理 3 对于 $\mathfrak{p}\in\operatorname{Spec}R$, $R_\mathfrak{p}$ 是局部环, 并且 $\mathfrak{m}=\left\{\frac{a}{s}\,\middle|\,a\in\mathfrak{p},s\in R-\mathfrak{p}\right\}$ 是 $R_\mathfrak{p}$ 的唯一极大理想.

证明 我们先来证明引理中等式的右边即是 $R_\mathfrak{p}-U(R_\mathfrak{p})$. (注意: 若 $\frac{a}{s}=\frac{b}{t}\in R_\mathfrak{p}$, 易知 $a\in\mathfrak{p}\Longleftrightarrow b\in\mathfrak{p}$. 从而"$a\in\mathfrak{p}$"这个性质与 a/s 的代表元 $a\in R$ 和 $s\in S$ 的选取无关.) 如果 $a/s\in U(R_\mathfrak{p})$ ($a\in R$, $s\in S=R-\mathfrak{p}$), 则有 $b/t\in R_\mathfrak{p}$ 使得 $\frac{ab}{st}=\frac{1}{1}$. 于是有 $u\in R-\mathfrak{p}$ 使得 $u(ab-st)=0$, 即 $u(ab)=stu$. 由于 s,t,u 均不属于 $\mathfrak{p}$, 从而 stu 也如此, 即 $uab\notin\mathfrak{p}$. 于是 $a\notin\mathfrak{p}$. 即 $a\in R-\mathfrak{p}$.

反之若 $a/s\in R_\mathfrak{p}$ 并且 $a,s\in R-\mathfrak{p}$，则 $s/a\in R_\mathfrak{p}$，于是由 $\frac{a}{s}\cdot\frac{s}{a}=\frac{1}{1}$ 可知 $a/s\in U(R_\mathfrak{p})$. 这就证明了 $U(R_\mathfrak{p})=\left\{\frac{a}{s}\in R_\mathfrak{p}\,\middle|\, s,\ a\in R-\mathfrak{p}\right\}$. 从而 $R_\mathfrak{p}-U(R_\mathfrak{p})=\left\{\frac{a}{s}\in R_\mathfrak{p}\,\middle|\, s\in R-\mathfrak{p}, a\in\mathfrak{p}\right\}$.

根据第一章的定理 3，为了证明 $R_\mathfrak{p}$ 是局部环，我们只需证明 $R_\mathfrak{p}-U(R_\mathfrak{p})$ 是 $R_\mathfrak{p}$ 的真理想即可. 而这件事是显然的. 从而 $R_\mathfrak{p}$ 为局部环，并且 $\mathfrak{m}=R_\mathfrak{p}-U(R_\mathfrak{p})$ 是它的唯一极大理想. ▌

下一个目标是考虑在环同态 $f: R\rightarrow S^{-1}R$, $a\mapsto\frac{a}{1}$ 之下，R 和 $S^{-1}R$ 之间理想的限制和扩张的一些特殊性质. 根据定义，若 $\mathfrak{a}$ 为 R 的理想，则 $\mathfrak{a}^e=f(\mathfrak{a})\cdot S^{-1}R$. 而对于 $S^{-1}R$ 中的理想 $\mathfrak{b}$, $\mathfrak{b}^c=f^{-1}(\mathfrak{b})$. 今后我们讨论 R 和 $S^{-1}R$ 之间的理想的限制和扩张均是指对于环同态 f 而言.

定理 1 设 S 是环 R 的乘法集. 则

(1) 对于 R 的每个理想 $\mathfrak{a}$, $\mathfrak{a}^e=\left\{\frac{a}{s}\,\middle|\, a\in\mathfrak{a}, s\in S\right\}$（右边可写成 $S^{-1}\mathfrak{a}$）.

(2) $S^{-1}R$ 中每个理想 $\mathfrak{b}$ 均是 R 中某个理想的扩张. 事实上，令 $\mathfrak{a}=\mathfrak{b}^c$，则 $\mathfrak{b}=\mathfrak{a}^e$.

(3) $\mathfrak{a}^{ec}=\bigcup\limits_{s\in S}(\mathfrak{a}:s)$.

(4) $\mathfrak{a}^e=S^{-1}R\Longleftrightarrow\mathfrak{a}\cap S\neq\varnothing$.

(5) $\mathfrak{a}$ 为 $S^{-1}R$ 中某理想的限制 $\Longleftrightarrow S$ 中每个元素在 $R/\mathfrak{a}$ 中的象均不是 $R/\mathfrak{a}$ 中的零因子.

(6) $S^{-1}R$ 中素理想一一保序对应于 R 中与 S 不相交的素理想.

证明 (1) 若 $a/s\in S^{-1}\mathfrak{a}$，即 $a\in\mathfrak{a}$，$s\in S$，则 $\frac{a}{s}=\frac{a}{1}\cdot\frac{1}{s}\in$

$f(\mathfrak{a})\cdot S^{-1}R=\mathfrak{a}^e$. 从而 $S^{-1}\mathfrak{a}\subseteq\mathfrak{a}^e$. 反之,$\mathfrak{a}^e$ 中每个元素均可表成有限和

$$\sum_{i=1}^{n}\frac{a_i}{1}\cdot\frac{b_i}{s_i}=\sum_{i=1}^{n}\frac{a_ib_i}{s_i}\qquad(a_i\in\mathfrak{a},b_i\in R,s_i\in S).$$

将右边"通分"(即化成公分母 $s=s_1s_2\cdots s_n$)然后相加,即知它属于 $S^{-1}\mathfrak{a}$. 于是 $\mathfrak{a}^e\subseteq S^{-1}\mathfrak{a}$. 从而 $\mathfrak{a}^e=S^{-1}\mathfrak{a}$.

(2)令 $\mathfrak{a}=\mathfrak{b}^c=f^{-1}(\mathfrak{b})$. 由第一章习题3可知 $\mathfrak{a}^e=S^{-1}\mathfrak{a}=\mathfrak{b}^{ce}\subseteq\mathfrak{b}$ 总是成立的. 另一方面,如果 $x/s\in\mathfrak{b}$,则 $\frac{x}{1}=\frac{x}{s}\cdot\frac{s}{1}\in\mathfrak{b}$.从而 $x=f^{-1}\left(\frac{x}{1}\right)\in\mathfrak{b}^c=\mathfrak{a}$. 于是 $x/s\in S^{-1}\mathfrak{a}$. 从而 $\mathfrak{b}\subseteq S^{-1}\mathfrak{a}=\mathfrak{a}^e$. 即 $\mathfrak{b}=\mathfrak{a}^e$.

(3)如果 $x\in\mathfrak{a}^{ec}=(S^{-1}\mathfrak{a})^c$,则 $\frac{x}{1}=\frac{a}{s}$,其中 $a\in\mathfrak{a},s\in S$. 于是有 $t\in S$ 使得 $t(xs-a)=0$,从而 $x(st)=at\in\mathfrak{a}$. 但是 $st\in S$,从而 $x\in(\mathfrak{a}:st)\subseteq\bigcup_{s\in S}(\mathfrak{a}:s)$. 反之,若 $x\in\bigcup_{s\in S}(\mathfrak{a}:s)$,则有 $s\in S$ 使得 $xs=a\in\mathfrak{a}$. 于是 $1\cdot(xs-a)=0$. 由于 $1\in S$,从而 $\frac{x}{1}=a/s\in S^{-1}\mathfrak{a}$. 于是 $x\in(S^{-1}\mathfrak{a})^c=\mathfrak{a}^{ec}$. 这就证明了 $\mathfrak{a}^{ec}=\bigcup_{s\in S}(\mathfrak{a}:s)$.

(4)显然 $R^e=S^{-1}R$, $(S^{-1}R)^c=f^{-1}(S^{-1}R)=R$. 于是由(3)即知:

$$\mathfrak{a}^e=S^{-1}R\Longleftrightarrow\mathfrak{a}^{ec}=R\Longleftrightarrow 1\in\bigcup_{s\in S}(\mathfrak{a}:s)\Longleftrightarrow\text{存在 } s\in S \text{ 使得 } s\in\mathfrak{a}\Longleftrightarrow\mathfrak{a}\cap S\neq\varnothing.$$

(5)由于 $\mathfrak{a}^{ec}\supseteq\mathfrak{a}$ 总是对的. 因此

$\mathfrak{a}$ 为 $S^{-1}R$ 中某理想的限制 $\Longleftrightarrow \mathfrak{a}^{ec}=\mathfrak{a} \Longleftrightarrow \mathfrak{a}^{ec}\subseteq \mathfrak{a}$

$\Longleftrightarrow \bigcup_{s\in S}(\mathfrak{a}:s)\subseteq \mathfrak{a}$

$\Longleftrightarrow$ 若 $x\in R, s\in S, xs\in \mathfrak{a}$，则 $x\in \mathfrak{a}$.

$\Longleftrightarrow$ 若 $s\in S, x\in R, \bar{x}\bar{s}=\bar{0}\in R/\mathfrak{a}$，则 $\bar{x}=\bar{0}\in R/\mathfrak{a}$.

$\Longleftrightarrow S$ 中每个元素在 $R/\mathfrak{a}$ 中的象均不是 $R/\mathfrak{a}$ 中的零因子.

(6)定义两个集合

$$C=\{\mathfrak{p}\in \operatorname{Spec}R \mid \mathfrak{p}\cap S=\varnothing\}, \qquad E=\operatorname{Spec}S^{-1}R.$$

如果 $\mathfrak{q}\in E$. 我们由§1.2习题9已知 $\mathfrak{q}^c=\mathfrak{p}\in \operatorname{Spec}R$，并且 $\mathfrak{p}\cap S=\varnothing$（因为若 $\mathfrak{p}\cap S\neq\varnothing$，则由(4)知 $\mathfrak{q}\supseteq\mathfrak{q}^{ce}=\mathfrak{p}^e=S^{-1}R$，与 $\mathfrak{q}$ 为素理想矛盾）. 于是我们有映射

$$f: E\to C, \quad \mathfrak{q}\mapsto\mathfrak{q}^c.$$

反之，如果 $\mathfrak{p}\in \operatorname{Spec}R$ 并且 $\mathfrak{p}\cap S=\varnothing$. 我们来证 $\mathfrak{p}^e=S^{-1}\mathfrak{p}\in \operatorname{Spec} S^{-1}R$. 首先由 $\mathfrak{p}\cap S=\varnothing$ 可知 $S^{-1}\mathfrak{p}\neq S^{-1}R$. 此外，假设 $\frac{ab}{st}=\frac{a}{s}\cdot\frac{b}{t}\in S^{-1}\mathfrak{p}$，则 $ab\in\mathfrak{p}$. 从而 a 或 $b\in\mathfrak{p}$. 于是 a/s 或 $b/t\in S^{-1}\mathfrak{p}$. 这就证明了 $S^{-1}\mathfrak{p}\in \operatorname{Spec}S^{-1}R$. 于是我们又有映射

$$g: C\to E, \quad \mathfrak{p}\mapsto S^{-1}\mathfrak{p}=\mathfrak{p}^e.$$

由(2)知 E 中素理想 $\mathfrak{p}$ 均是扩张理想. 即存在 R 中理想 $\mathfrak{a}$ 使得 $\mathfrak{q}=\mathfrak{a}^e$. 于是 $gf(\mathfrak{q})=\mathfrak{q}^{ce}=\mathfrak{a}^{ece}=\mathfrak{a}^e=\mathfrak{q}$. 这表明 $gf=1_E$. 另一方面，如果 $\mathfrak{p}\in C$，即 $\mathfrak{p}\in \operatorname{Spec}R$ 并且 $\mathfrak{p}\cap S=\varnothing$，则由(3)我们有

$$fg(\mathfrak{p})=\mathfrak{p}^{ec}=\bigcup_{s\in S}(\mathfrak{p}:s)=\mathfrak{p}\ (\text{最后等式用到 } \mathfrak{p}\cap S=\varnothing).$$

从而 $fg=1_C$. 这就表明 f 和 g 为互逆映射. 从而集合 C 和 E 是一一对应的. 而 f 和 g 的保序性是显然的. ▌

在定理1的(6)中取 $S=R-\mathfrak{p}$，$\mathfrak{p}\in \operatorname{Spec}R$. 则对于 R 中每个

集合 T，$T\cap S=\varnothing\Longleftrightarrow T\subseteq\mathfrak{p}$. 从而直接得到

系 1 设 $\mathfrak{p}\in\mathrm{Spec}R$，则 $R_{\mathfrak{p}}$ 中素理想和 R 中包含于 $\mathfrak{p}$ 之内的素理想是一一保序对应的. ▌

注记 (1)在系 1 的保序对应之下，R 中素理想 $\mathfrak{p}$ 显然对应于 $R_{\mathfrak{p}}$ 的唯一极大理想 $\mathfrak{m}=S^{-1}\mathfrak{p}(S=R-\mathfrak{p})$.

(2) 系 1 给出一个重要的原则：如果我们在某个问题中只需考虑环 R 中包含在 $\mathfrak{p}$ 之内的素理想，那末通过局部化可以去考虑更为简单的环 $R_{\mathfrak{p}}$ 的素谱 $\mathrm{Spec}\,R_{\mathfrak{p}}$. 因为这两者之间是保序一一对应的. 另一方面，如果我们只想考虑环 R 中包含 $\mathfrak{p}$ 的那些素理想，请转向商环 $R/\mathfrak{p}$. 因为根据环的同态基本定理，R 中包含 $\mathfrak{p}$ 的素理想与 $R/\mathfrak{p}$ 中的素理想是保序一一对应的.

现在给出利用局部化方法研究环论问题的第一个例子. 设 $f:A\to B$ 为环同态，则对每个 $\mathfrak{q}\in\mathrm{Spec}\,B$，$\mathfrak{q}^c=f^{-1}(\mathfrak{q})$ 必是 A 中的素理想. 但是反过来，A 中素理想不一定是 B 中某个素理想的限制.

系 2 设 $f:A\to B$ 为环的同态，$\mathfrak{p}\in\mathrm{Spec}\,A$. 则 $\mathfrak{p}$ 是 B 中某个素理想的限制 $\Longleftrightarrow\mathfrak{p}^{ec}=\mathfrak{p}$.

证明 $\Rightarrow$：设 $\mathfrak{q}\in\mathrm{Spec}\,B$，$\mathfrak{p}=\mathfrak{q}^c$，则 $\mathfrak{p}^{ec}=\mathfrak{q}^{cec}=\mathfrak{q}^c=\mathfrak{p}$.

$\Leftarrow$：记 $S=f(A-\mathfrak{p})$，容易验证这是 B 的乘法集(乘法集的环同态象必为乘法集). 由 $\mathfrak{p}^{ec}=\mathfrak{p}$ 可知 $\mathfrak{p}^e\cap S=\varnothing$. (因为如果有 $x\in\mathfrak{p}^e\cap S$，则有 $y\in A-\mathfrak{p}$ 使得 $x=f(y)$. 从而 $y\in f^{-1}(x)\subseteq f^{-1}(\mathfrak{p}^e)=\mathfrak{p}^{ec}=\mathfrak{p}$. 而这与 $y\in A-\mathfrak{p}$ 矛盾.)所以根据定理1的(4)，$\mathfrak{p}^e$ 在 $S^{-1}B$ 中的扩张 $\mathfrak{n}$ 是 $S^{-1}B$ 的真理想. 于是 $\mathfrak{n}$ 包含在 $S^{-1}B$ 的某个极大理想 $\mathfrak{m}$ 之中，以 $\mathfrak{q}$ 表示 $\mathfrak{m}$ 在 B 中的限制，$\mathfrak{q}^c$ 表示 $\mathfrak{q}$ 在 A 中的限制. 则 $\mathfrak{m}\supseteq\mathfrak{n}\Rightarrow\mathfrak{q}=\mathfrak{m}$ 在 B 中的限制 $\supseteq\mathfrak{n}$ 在 B 中的限制 $\supseteq\mathfrak{p}^e$ (参考图示) $\Rightarrow\mathfrak{q}^c\supseteq\mathfrak{p}^{ec}\supseteq\mathfrak{p}$.

$$A\to B\to S^{-1}B$$

$$\begin{array}{ccc} \mathfrak{p}\mapsto\mathfrak{p}^e\mapsto\mathfrak{n} & & \\ \quad\quad\quad\quad\cap\!\!| & & \left(\begin{array}{l}\mapsto\text{：扩充}\\ \leftarrow\!\!\dashv\text{：限制}\end{array}\right) \\ \mathfrak{q}^c\leftarrow\!\!\dashv\mathfrak{q}\leftarrow\!\!\dashv\mathfrak{m} & & \end{array}$$

另一方面，由于 $\mathfrak{q}$ 是极大理想 $\mathfrak{m}$ 的限制，从而由定理 1 的(6)可知 $\mathfrak{q}$ 为 B 的素理想并且 $\mathfrak{q}\cap S=\varnothing$. 由于 $S=f(A-\mathfrak{p})$，从而 $f(A)\cap\mathfrak{q}\subseteq f(\mathfrak{p})$. 于是 $\mathfrak{q}^c=f^{-1}(\mathfrak{q})\subseteq f^{-1}(f(\mathfrak{p}))\subseteq\mathfrak{p}^{ec}=\mathfrak{p}$. 从而 $\mathfrak{q}^c=\mathfrak{p}$ 而 $\mathfrak{q}\in\operatorname{Spec}B$. ▌

习 题

1. 设 S 为环 R 的乘法集. 则(1) $S^{-1}R=0\Longleftrightarrow 0\in S$. (2) $S^{-1}R=R\Longleftrightarrow S\subseteq U(R)$.

2. 设 S 为环 R 的乘法集，$\mathfrak{a}$ 为 R 的理想，则

(1) $\sqrt{S^{-1}\mathfrak{a}}=S^{-1}\sqrt{\mathfrak{a}}$.

(2) $S^{-1}N(R)=N(S^{-1}R)$(其中 $N(R)$ 表示环 R 的小根).

3. 设 $\mathfrak{a}$ 为环 R 的理想. 求证 $S=1+\mathfrak{a}=\{1+a\,|\,a\in\mathfrak{a}\}$ 是 R 的乘法集，并且 $S^{-1}\mathfrak{a}\subseteq r(S^{-1}R)$($S^{-1}R$ 的大根).

4. 设 S 和 T 是环 R 的两个乘法集. U 为 T 在 $S^{-1}R$ 中的象(对于 $f:R\to S^{-1}R$, $a\mapsto a/1$). 求证有环同构 $(ST)^{-1}R\cong U^{-1}(S^{-1}R)$(其中 $ST=\{st\,|\,s\in S, t\in T\}$).

5. 设 R 为非零环，$\Sigma=\{R$ 的乘法集 $S\,|\,0\notin S\}$. 求证集合 Σ(对于包含关系)有极大元. 并且，S 为 Σ 的极大元 $\Longleftrightarrow R-S$ 为 R 的极小素理想.

6. 环 R 的乘法集 S 叫作是**饱和的**，是指：若 $xy\in S$，则 $x\in S$ 并且 $y\in S$. 求证

(1) S 为饱和乘法集 $\Longleftrightarrow R-S$ 是一些素理想之并，

(2) 对于每个乘法集 S，求证有唯一的包含 S 的最小饱和乘法集 $\bar{S}$，并且 $\bar{S}=R-\bigcup\limits_{\substack{\mathfrak{p}\in\operatorname{Spec}R\\ \mathfrak{p}\cap S=\varnothing}}\mathfrak{p}$.

(3) 设 $\mathfrak{a}$ 为环 R 的理想，$S=1+\mathfrak{a}$，试问 $\bar{S}$ 为何?

7. 设 S 和 T 均为环 R 的乘法集，并且 $S\subseteq T$. 令

$$\varphi: S^{-1}R \to T^{-1}R, \varphi(a/s) = a/s (a \in R, s \in S)$$

(这是环同态)．求证下面五个命题彼此等价：

(1) φ为环同构．

(2) 对每个 $t \in T, t/1 \in U(S^{-1}R)$.

(3) 对每个 $t \in T$，均有 $x \in R$ 使得 $xt \in S$.

(4) $T \subseteq \bar{S}$ ($\bar{S}$ 见习题 6)．

(5) 若 $\mathfrak{p} \in \mathrm{Spec}R, \mathfrak{p} \cap T \neq \varnothing$，则 $\mathfrak{p} \cap S \neq \varnothing$.

8．以 S_0 表示R中不是零因子的元素全体．求证：

(1) S_0 为R的饱和乘法集． 从而R的零因子集合D是R的一些素理想之并．

(2) R的每个极小素理想均包含在D之中．[提示：利用习题 5．]

9．S_0 如上题所示，我们称 $S_0^{-1}R$ 为 R 的**全分式环**．求证：

(1) S_0 是R的最大乘法集 S 使得$f: R \to S^{-1}R, a \mapsto a/1$ 为单射．

(2) $S_0^{-1}R$ 中的元素或者为零因子，或者为单位．

(3) 如果环R中非单位均是零因子，则 $R \cong S_0^{-1}R$（环同构)．

10．设$f: A \to B$ 为环的同态，考虑映射

$$f^*: \mathrm{Spec}\, B \to \mathrm{Spec} A, f^*(\mathfrak{q}) = f^{-1}(\mathfrak{q}).$$

求证：

(1) A中素理想均为 B 中某个素理想（对于f）的限制 $\Longleftrightarrow f^*$ 为满射．

(2) B中素理想均为A中某个素理想(对于f)的扩张$\Rightarrow f^*$ 为单射．

(3) 试问(2)中$\Leftarrow$是否成立？

11．(1) 对于 $R = \mathbf{Z}, S = 2\mathbf{Z}^*$，求证 $S^{-1}R = \mathbf{Q}$.

(2) 试给出具有性质“$S^{-1}\mathbf{Z} = \mathbf{Q}$”的 $\mathbf{Z}$ 中乘法集 S 的一个刻画．

12．设S为环R的乘法集，$0 \notin S$．求证：

(1) R为整环$\Rightarrow S^{-1}R$ 为整环．

(2) R为主理想整环$\Rightarrow S^{-1}R$为主理想整环．

(3) R为唯一因子分解整环$\Rightarrow S^{-1}R$为唯一因子分解整环．

13．设S为环R的乘法集，$0 \notin S$．如果 $S^{-1}R$为整环， 则R是否必为整环？[提示：考虑$R = \mathbf{Z}/6\mathbf{Z}, S = \{\bar{2}, \bar{4}\}$．]

14．设 $\mathfrak{m}$ 为环 R 的极大理想，$n\geqslant 1$．求证商环 $R/\mathfrak{m}^n$ 只有一个素理想（从而为局部环）．

15．设 $f: A\to B$ 是环的同态，$f(A)\neq 0$．如果 A 为局部环，则 B 也是局部环．

16．设 $\mathfrak{p}\in \mathrm{Spec} R$，$\mathfrak{m}$ 为 $R_\mathfrak{p}$ 中唯一极大理想．求证域 $R_\mathfrak{p}/\mathfrak{m}$ 同构于整环 $R/\mathfrak{p}$ 的商域．

17．设 $\mathfrak{p}$ 为环 R 的极小素理想，$a\in\mathfrak{p}$．求证有 $s\in R-\mathfrak{p}$，$k\geqslant 1$，使得 $sa^k=0$．

18．设 A 为环，$\mathfrak{p}_1,\cdots,\mathfrak{p}_n\in \mathrm{Spec} A$．求证：

(1) $S=\bigcap\limits_{i=1}^{n}(A-\mathfrak{p}_i)=A-\bigcup\limits_{i=1}^{n}\mathfrak{p}_i$ 为 A 的乘法集。

(2) $S^{-1}A$ 为半局部环，更确切地说：$\mathrm{Max}(S^{-1}A)=\{S^{-1}\mathfrak{q}\mid \mathfrak{q}$ 为集合 $\{\mathfrak{p},\cdots,\mathfrak{p}_n\}$ 的极大元$\}$．

(3) $A_{\mathfrak{p}_i}\cong(S^{-1}A)_{S^{-1}\mathfrak{p}_i}$（环同构）．

(4) 若 A 为整环，则 $S^{-1}A=\bigcap\limits_{i=1}^{n}A_{\mathfrak{p}_i}$（两边均在 A 的商域 K 之中）．

§3.2 分式模

现在我们谈分式模和模的局部化．设 S 是环 R 的乘法集，M 为 R-模．我们在集合 $M\times S$ 上定义如下的二元关系：对于 $(m,s),(m',s')\in M\times S$，

$$(m,s)\sim(m',s')\Longleftrightarrow \text{存在 } u\in S \text{ 使得 } u(s'm-sm')=0.$$

这是等价关系．以 m/s 表示 (m,s) 所在的等价类，$S^{-1}M$ 表示全部等价类组成的集合．在 $S^{-1}M$ 中定义加法为：

$$\frac{m}{s}+\frac{n}{t}=\frac{tm+sn}{st}\quad(m,n\in M,s,t\in S).$$

可以证明此定义与等价类中代表元的选取无关，并且 $S^{-1}M$ 由此而成为 Abel 群．零元素为 $\frac{0}{1}$．进而，对于 $\frac{a}{s}\in S^{-1}R$ $(a\in R,$

$s\in S$)和 $\frac{m}{t}\in S^{-1}M(m\in M, t\in S)$定义

$$\frac{a}{s}\cdot\frac{m}{t}=\frac{am}{st}\in S^{-1}M.$$

可以证明此定义也与等价类中代表元的选取无关，并且 $S^{-1}M$ 由此而成为 $S^{-1}R$-模. 我们把这个 $S^{-1}R$-模 $S^{-1}M$ 叫作是 R-模 M对于R的乘法集S的**分式模**.

例 1 分式环 $S^{-1}R$ 是分式模的特殊情形，即 $S^{-1}R$ 是 R-模 R对于S的分式模.

例 2 设 $\mathfrak{a}$ 为环R的理想，S 是R的乘法集. 则 R-模 $\mathfrak{a}$ 对于 S 的分式模为 $S^{-1}\mathfrak{a}=\left\{\frac{a}{s}\in S^{-1}R \mid a\in\mathfrak{a}, s\in S\right\}$. 这与§ 3.1 中定理 1 中符号 $S^{-1}\mathfrak{a}$（那里表示 $\mathfrak{a}$ 到 $S^{-1}R$ 中的扩张理想）是一致的.

例 3 对于最重要的情形：$S=R-\mathfrak{p}$, $\mathfrak{p}\in\mathrm{Spec}R$. 我们把$R_{\mathfrak{p}}$-模 $S^{-1}M$ 记成 $M_{\mathfrak{p}}$，叫作是 **M 在 $\mathfrak{p}$ 处的局部化.**

类似于分式环的情形(引理 1)可以证明：$f: M\to S^{-1}M$, $m\mapsto m/1$ 为 R-模同态，并且 $\mathrm{Ker}f=\{m\in M \mid$ 有 $s\in S$ 使得 $sm=0\}$.

设 $f: M\mapsto N$ 为 R-模同态，S 为R的乘法集. 定义映射

$$S^{-1}f: S^{-1}M\to S^{-1}N, \quad \frac{m}{s}\mapsto\frac{f(m)}{s}.$$

直接验证这是 $S^{-1}R$-模同态. 并且如果 $g: N\to P$ 也是 R-模同态，则 $S^{-1}(gf)=(S^{-1}g)(S^{-1}f)$.

定理 2 S^{-1}是正合算子. 确切地说，如果$\mathscr{E}$：$M'\xrightarrow{f}M\xrightarrow{g}M''$ 为 R-模正合序列，则$S^{-1}(\mathscr{E})$：$S^{-1}M'\xrightarrow{S^{-1}f}S^{-1}M\xrightarrow{S^{-1}g}S^{-1}M''$ 是 $S^{-1}R$-模正合序列.

证明 由 $gf=0$ 可知 $S^{-1}g\cdot S^{-1}f=S^{-1}(gf)=S^{-1}(0)=0$. 从而 $\mathrm{Im}(S^{-1}f)\subseteq\mathrm{Ker}(S^{-1}g)$. 反之,若 $\frac{m}{s}\in\mathrm{Ker}(S^{-1}g)$,则 $\frac{g(m)}{s}=\frac{0}{1}\in S^{-1}M''$. 于是有 $t\in S$ 使得 $tg(m)=0\in M''$. 但是 g 为 R-模同态,从而 $g(tm)=0$. 于是 $tm\in\mathrm{Ker}g=\mathrm{Im}f$. 即有 $m'\in M'$,使得 $tm=f(m')$. 从而在 $S^{-1}M$ 中有 $\frac{m}{s}=\frac{f(m')}{st}=(S^{-1}f)\left(\frac{m'}{st}\right)\in\mathrm{Im}(S^{-1}f)$. 于是 $\mathrm{Ker}(S^{-1}g)\subseteq\mathrm{Im}(S^{-1}f)$. ▌

注记 特别地,若 M' 为 M 的 R-子模,则 $S^{-1}M'$ 可看成是 $S^{-1}M$ 的 $S^{-1}R$-子模.

引理 4 设 N 和 P 均为 R-模 M 的子模, S 为 R 的乘法集. 则

(1) $S^{-1}(N+P)=S^{-1}N+S^{-1}P$;

(2) $S^{-1}(N\cap P)=S^{-1}N\cap S^{-1}P$;

(3) 有 $S^{-1}R$-模同构: $S^{-1}(M/N)\cong S^{-1}M/S^{-1}N$.

证明 (1) 设 $x\in S^{-1}(N+P)$,则 $x=\frac{n+p}{s}(n\in N,p\in P,s\in S)$. 但是 $\frac{n}{s}+\frac{p}{s}=\frac{sn+sp}{s^2}=\frac{s}{s}\cdot\frac{n+p}{s}=\frac{1}{1}\cdot\frac{n+p}{s}=\frac{n+p}{s}=x$, 因此 $x\in S^{-1}N+S^{-1}P$. 反之,若 $x\in S^{-1}N+S^{-1}P$,则 $x=\frac{n}{s}+\frac{p}{t}(n\in N,p\in P,s,\ t\in S)$. 从而 $x=\frac{tn+sp}{st}\in S^{-1}(N+P)$ (因为 $tn\in N,sp\in P,st\in S$).

(2) 设 $x\in S^{-1}N\cap S^{-1}P$,则 $x=\frac{n}{s}=\frac{p}{t}(n\in N,p\in P,s,t\in S)$. 于是有 $u\in S$ 使得 $u(tn-sp)=0$. 令 $w=utn=usp$, 则

$w\in N\cap P$，而$x=\frac{n}{s}=\frac{w}{ust}\in S^{-1}(N\cap P)$. 反之，若 $x\in S^{-1}(N\cap P)$，则显然有 $x\in S^{-1}N\cap S^{-1}P$.

(3) R-模短正合序列 $0\to N\to M\to M/N\to 0$ 经正合算子 S^{-1} 的作用（定理 2）给出 $S^{-1}R$-模短正合序列 $0\to S^{-1}N\to S^{-1}M\to S^{-1}(M/N)\to 0$. 从而有 $S^{-1}R$-模同构 $S^{-1}M/S^{-1}N\cong S^{-1}(M/N)$. ▌

注记 引理 4 的 (1) 可以推广到任意多个子模之和的情形：$S^{-1}\left(\sum_{i\in I}N_i\right)=\sum_{i\in I}(S^{-1}N_i)$. 证明是一样的.

环R中的理想 $\mathfrak{a}$ 自然地看成是R-模. 如果S为R的乘法集，则 R-模 $\mathfrak{a}$ 对于 S 的分式模为 $S^{-1}\mathfrak{a}$. 这是 $S^{-1}R$-模. 从而为 $S^{-1}R$的理想. 由引理 4 直接推出

系 1 设 $\mathfrak{a}$ 和 $\mathfrak{b}$ 为环R的理想，S为R的乘法集. 则

(1) 在环 $S^{-1}R$中，$S^{-1}(\mathfrak{a}+\mathfrak{b})=S^{-1}\mathfrak{a}+S^{-1}\mathfrak{b}$.

(2) 在环 $S^{-1}R$中，$S^{-1}(\mathfrak{a}\cap\mathfrak{b})=S^{-1}\mathfrak{a}\cap S^{-1}\mathfrak{b}$.

(3) 以 $\bar{S}$ 表示S在商环$R/\mathfrak{a}$中之象. 则有环同构：$\bar{S}^{-1}(R/\mathfrak{a})\cong S^{-1}R/S^{-1}\mathfrak{a}$.

下一个定理反映了算子 S^{-1} 和$\otimes$之间的联系.

定理 3 设S为环R的乘法集，M 为 R-模. 则有 $S^{-1}R$-模同构：$S^{-1}M\cong S^{-1}R\otimes_R M$. 确切地说，存在唯一的$S^{-1}R$-模同构 $f:S^{-1}R\otimes_R M\cong S^{-1}M$，使得

$$f\left(\frac{a}{s}\otimes m\right)=\frac{am}{s}\ (a\in R,s\in S,m\in M). \qquad (1)$$

证明 由标准同态 $R\to S^{-1}R$ 将 $S^{-1}M$ 看成是 R-模. 直接验证映射

$$S^{-1}R \times M \to S^{-1}M,\ \left(\frac{a}{s}, m\right) \mapsto \frac{am}{s}$$

是 R-双线性映射. 从而第一章定理 10 诱导出 R-模同态 $f: S^{-1}R \otimes_R M \to S^{-1}M$ 使得(1)式成立. 由(1)式容易看出 f 事实上为 $S^{-1}R$-模同态,并且显然是满同态. 而且由条件(1)所唯一决定. 最后只需再证 f 为单射. 由于

$$\sum_{i=1}^{n}\left(\frac{a_i}{s_i} \otimes m_i\right) = \sum_{i=1}^{n} \frac{a_i t_i}{s} \otimes m_i = \sum_{i=1}^{n} \frac{1}{s} \otimes a_i t_i m_i = \frac{1}{s} \otimes \sum_{i=1}^{n} a_i t_i m_i,$$

其中 $s = s_1 \cdots s_n, t_i = s/s_i$. 从而 $S^{-1}R \otimes_R M$ 中元素均可表成 $\frac{1}{s} \otimes m$ 的形式($s \in S, m \in M$). 如果 $f\left(\frac{1}{s} \otimes m\right) = 0$,则 $\frac{m}{s} = \frac{0}{1}$. 于是有 $t \in S$ 使得 $tm = 0$. 从而 $\frac{1}{s} \otimes m = \frac{t}{st} \otimes m = \frac{1}{st} \otimes tm = \frac{1}{st} \otimes 0 = 0$. 这表明 f 为单射. ▌

由定理 2 和定理 3 立刻得到

系 1 $S^{-1}R$ 为平坦 R-模. ▌

定理 2 表明 S^{-1} 保持模序列的正合性, 引理 4 表明 S^{-1} 与模的许多运算都可以交换,下面系 2 表明 S^{-1} 保持模的自由性,有限生成性和投射性. 我们在下章还要证明 S^{-1} 保持模的 Noether 性. 在上节习题中我们还看到 S^{-1} 保持环的许多性质. 这一切表明算子 S^{-1} 具有极好的性状.

系 2 设 S 为环 R 的乘法集. 则

(1) M 为自由 R-模 $\Rightarrow S^{-1}M$ 为自由 $S^{-1}R$-模.

(2) M 为有限生成 R-模 $\Rightarrow S^{-1}M$ 为有限生成 $S^{-1}R$-模.

(3) M 为投射 R-模 $\Rightarrow S^{-1}M$ 为投射 $S^{-1}R$-模.

证明 (1) 若 $M = \bigoplus_{i \in I} R_i, R_i \cong R$. 则由定理 3 可知

$$S^{-1}M \cong S^{-1}R\otimes_R(\bigoplus_{i\in I} R_i) \cong \bigoplus_{i\in I}(S^{-1}R\otimes_R R_i).$$

但是 $S^{-1}R\otimes_R R_i \cong S^{-1}R\otimes_R R\cong S^{-1}R$. 从而 $S^{-1}M$ 同构于 $|I|$ 个 $S^{-1}R$ 的直和,即为自由 $S^{-1}R$-模.

(2) 若 M 为有限生成 R-模,则存在秩有限的自由 R-模 F, 使得 $F\to M\to 0$ 是 R-模正合序列. 作用正合算子 S^{-1} 之后得到 $S^{-1}R$-模正合序列 $S^{-1}F\to S^{-1}M\to 0$. 由(1)知 $S^{-1}F$ 为秩有限的自由 $S^{-1}R$-模,从而它的商模 $S^{-1}M$ 是有限生成的.

(3) 若 M 为投射 R-模,则有自由 R-模 F 和 R-模 N 使得 $F\cong M\oplus N$. 于是由定理 3 可知

$$\begin{aligned} S^{-1}F &\cong S^{-1}R\otimes_R F\cong S^{-1}R\otimes_R(M\oplus N)\\ &\cong(S^{-1}R\otimes_R M)\oplus(S^{-1}R\otimes_R N)\\ &\cong S^{-1}M\oplus S^{-1}N. \end{aligned}$$

由于 $S^{-1}F$ 是自由 $S^{-1}R$-模, 从而它的直和成分 $S^{-1}M$ 是投射 $S^{-1}R$-模. ▌

定理 4 设 M,N 为 R-模,则有唯一的 $S^{-1}R$-模同构

$$f: S^{-1}M\otimes_{S^{-1}R}S^{-1}N \xrightarrow{\sim} S^{-1}(M\otimes_R N),$$

使得 $f\left(\frac{m}{s}\otimes\frac{n}{t}\right)=\frac{m\otimes n}{st}(m\in M, n\in N, s,t\in S)$.

证明 仿照定理 3 的证明,留给读者练习. ▌

在定理 4 中取 $S=R-\mathfrak{p}$, $\mathfrak{p}\in\operatorname{Spec}R$ 就得到

系 设 $\mathfrak{p}\in\operatorname{Spec}R$,则对于 R-模 M,N,我们有 $R_\mathfrak{p}$-模同构: $M_\mathfrak{p}\otimes_{R_\mathfrak{p}}N_\mathfrak{p}\cong(M\otimes_R N)_\mathfrak{p}$. ▌

下面两个引理同样表明 S^{-1} 的良好性状.

引理 5 设 S 为 R 的乘法集, M 是有限生成 R-模. 则 $S^{-1}(\operatorname{Ann}(M))=\operatorname{Ann}(S^{-1}M)$(两边均是 $S^{-1}R$ 的理想).

证明 如果引理对 R-模 N 和 P 成立，即 $S^{-1}(\mathrm{Ann}(N))=\mathrm{Ann}(S^{-1}N)$, $S^{-1}(\mathrm{Ann}(P))=\mathrm{Ann}(S^{-1}P)$，则

$$
\begin{aligned}
S^{-1}(\mathrm{Ann}(N+P)) &= S^{-1}(\mathrm{Ann}(N)\cap\mathrm{Ann}(P)) \\
&= S^{-1}(\mathrm{Ann}(N))\cap S^{-1}(\mathrm{Ann}(P)) \\
&= \mathrm{Ann}(S^{-1}N)\cap\mathrm{Ann}(S^{-1}P) \\
&= \mathrm{Ann}(S^{-1}N+S^{-1}P)=\mathrm{Ann}(S^{-1}(N+P)).
\end{aligned}
$$

即引理对 $N+P$ 也成立. 由于有限生成 R-模是有限个循环 R-模的和，从而我们只需对 M 是循环 R-模的情形证明引理即可. 但是循环 R-模 M 均同构于 $R/\mathfrak{a}$, $\mathfrak{a}$ 为 R 的某个理想. 于是 $\mathrm{Ann}(M)=\mathrm{Ann}(R/\mathfrak{a})=\mathfrak{a}$. 由引理 4 的(3)我们有 $S^{-1}M\cong S^{-1}R/S^{-1}\mathfrak{a}$. 于是 $\mathrm{Ann}(S^{-1}M)=\mathrm{Ann}(S^{-1}R/S^{-1}\mathfrak{a})=S^{-1}\mathfrak{a}=S^{-1}(\mathrm{Ann}(M))$. ▌

引理 6 设 M 为 R-模, N 和 P 为 M 的 R-子模,并且 P 是有限生成 R-模. S 为 R 的乘法集. 则

$$S^{-1}(N:P)=(S^{-1}N:S^{-1}P).$$

(回忆:$(N:P)=\{a\in R\mid aP\subseteq N\}$ 是 R 的理想.)

证明 利用 $(N:P)=\mathrm{Ann}\left(\dfrac{N+P}{N}\right)$ 和引理 5. ▌

习 题

1. 设 S 为环 R 的乘法集, M 为有限生成 R-模,则 $S^{-1}M=0\Longleftrightarrow$ 有 $s\in S$ 使得 $sM=0$.

2. 设 $f:A\to B$ 为环同态，由此将 B 作成 A-模. 令 S 为环 A 的乘法集，$T=f(S)$. 求证有 $S^{-1}A$-模同构: $S^{-1}B\cong T^{-1}B$.

3. 设 R 为整环, K 为 R 的商域, M 为 R-模. 定义 R-模同态 $f:M\to K\otimes_R M$, $m\mapsto 1\otimes m$. 求证 $\mathrm{Ker}f=T(M)$.

4. 补足定理 4 的证明.

5. 设 S 是环 R 的乘法集. 如果 M 是平坦 R-模，求证 $S^{-1}M$ 是平坦

$S^{-1}R$-模.

6．设 $\mathfrak{m}$ 为环 R 的极大理想，M 为 R-模，$S=R-\mathfrak{m}$.

(1) 若 $s\in S$，求证对每个正整数 n，均有 $s^{-1}\in R$，使得 $s^{-1}\cdot s\equiv 1(\bmod \mathfrak{m}^n)$.

(2) 定义 $R_{\mathfrak{m}}\times M/\mathfrak{m}^n M\to M/\mathfrak{m}^n M$，$(a/s,\overline{m})\mapsto \overline{as^{-1}m}$.

其中 $a\in R, s\in S, s^{-1}\in R$ 使得 $s^{-1}\cdot s\equiv 1(\bmod\ \mathfrak{m}^n)$，$m\in M$，$\overline{m}$ 表示 m 在商模 $M/\mathfrak{m}^n M$ 中的象．求证这个映射是可定义的（即它不依赖于 s^{-1} 的不同选取方式），并且由此使 $M/\mathfrak{m}^n M$ 成为 $R_{\mathfrak{m}}$-模.

(3) 令 $\widetilde{\mathfrak{m}}=\mathfrak{m}R_{\mathfrak{m}}$，求证有 $R_{\mathfrak{m}}$-模同构 $M/\mathfrak{m}^n M\cong M_{\mathfrak{m}}/\widetilde{\mathfrak{m}}^n M_{\mathfrak{m}}$.

§3.3 局部性质

设 P 是环(或模)上的某个性质．如果对于每个环 R(或者每个 R-模 M)，

R(或 M)有性质 $P\Longleftrightarrow$ 对于每个 $\mathfrak{p}\in\operatorname{Spec}R$，$R_{\mathfrak{p}}$(或 $M_{\mathfrak{p}}$)均有性质 P.

我们就称 P 是一个**局部性质**．这样一来，如果 P 是一个局部性质．为了检验 R(或者 R-模 M)是否有性质 P，只需对每个局部化 $R_{\mathfrak{p}}$(或者 $M_{\mathfrak{p}}$)检验是否有性质 P 即可．由于 $R_{\mathfrak{p}}$(或 $M_{\mathfrak{p}}$)通常有比 R(或 M)简单的结构，因此后一个检验往往要容易得多．这就是局部化方法的好处.

有相当多的性质是局部性质．例如下面的引理 7 和引理 9 表明："M 为零模"和"M 为平坦 R-模"均是局部性质．引理 8 表明关于模同态的某些性质也是局部性质．在习题和以后几章中，我们还会见到更多的局部性质.

引理 7 设 M 为 R-模，则下面条件彼此等价：

(1) $M=0$；

(2) 对于每个 $\mathfrak{p}\in\operatorname{Spec}R$，$M_{\mathfrak{p}}=0$；

(3) 对于每个 $\mathfrak{m}\in\operatorname{Max}R$，$M_{\mathfrak{m}}=0$.

证明：(1)$\Rightarrow$(2)$\Rightarrow$(3) 显然. (3)$\Rightarrow$(1)：用反证法. 如果 $M\neq 0$，令 $0\neq m\in M$. 则 $1\notin \mathrm{Ann}(m)=\{r\in R\,|\,rm=0\}$. 从而 $\mathrm{Ann}(m)$是R的真理想. 于是它包含在某个极大理想 $\mathfrak{m}$之中. 但是 $M_{\mathfrak{m}}=0$，从而 $0=\dfrac{m}{1}\in M_{\mathfrak{m}}$. 于是有 $s\in S=R-\mathfrak{m}$ 使得 $sm=0$，从而 $s\in \mathrm{Ann}(m)\subseteq \mathfrak{m}$. 而这与 $s\in R-\mathfrak{m}$ 相矛盾. ▌

引理 8 设 $f:M\to N$ 为R-模同态. 对于每个$\mathfrak{p}\in \mathrm{Spec}R$，令 $f_{\mathfrak{p}}:M_{\mathfrak{p}}\to N_{\mathfrak{p}}$为 $R_{\mathfrak{p}}$-模同态，$f_{\mathfrak{p}}\left(\dfrac{m}{s}\right)=\dfrac{f(m)}{s}$ $(s\in R-\mathfrak{p})$. 则

(1) f 为单同态$\Longleftrightarrow$对每个 $\mathfrak{p}\in \mathrm{Spec}R$，$f_{\mathfrak{p}}$为单同态
$\Longleftrightarrow$对每个 $\mathfrak{m}\in \mathrm{Max}R$，$f_{\mathfrak{m}}$为单同态.

(2) f 为满同态$\Longleftrightarrow$对每个 $\mathfrak{p}\in \mathrm{Spec}R$，$f_{\mathfrak{p}}$为满同态
$\Longleftrightarrow$对每个 $\mathfrak{m}\in \mathrm{Max}R$，$f_{\mathfrak{m}}$为满同态.

(3) f 为 同 构$\Longleftrightarrow$对每个 $\mathfrak{p}\in \mathrm{Spec}R$，$f_{\mathfrak{p}}$为同构
$\Longleftrightarrow$对每个 $\mathfrak{m}\in \mathrm{Max}R$，$f_{\mathfrak{m}}$为同构.

证明 (1)对于每个R-模同态$f:M\to N$，我们有 R-模正合序列 $0\to K\to M\xrightarrow{f} N$，$K=\mathrm{Ker}f$. 从而对每个$\mathfrak{p}\in \mathrm{Spec}R$，我们有$R_{\mathfrak{p}}$-模正合序列$0\to K_{\mathfrak{p}}\to M_{\mathfrak{p}}\xrightarrow{f_{\mathfrak{p}}} N_{\mathfrak{p}}$ (定理 2). 于是，f 为单同态$\Longleftrightarrow$ $K=0$. $f_{\mathfrak{p}}$为单同态$\Longleftrightarrow K_{\mathfrak{p}}=0$. 然后再利用引理 7 即可证得 (1) 中诸条件的等价性.

(2) 利用 R-模正合序列 $M\xrightarrow{f} N\to N/\mathrm{Im}f\to 0$. 注意，$f$ 为满同态$\Longleftrightarrow N/\mathrm{Im}f=0$. 然后可象 (1) 一样地证明.

(3) 由 (1) 和 (2) 得出. ▌

引理 9 设 M 为 R-模，则下面三条件彼此等价：

(1) M为平坦 R-模；

(2) 对于每个 $\mathfrak{p}\in \mathrm{Spec}R$，$M_{\mathfrak{p}}$为平坦 $R_{\mathfrak{p}}$-模；

(3) 对于每个 $\mathfrak{m}\in \mathrm{Max}R$，$M_{\mathfrak{m}}$为平坦 $R_{\mathfrak{m}}$-模.

证明 (1)⇒(2)：设 $0\to N\xrightarrow{\varphi}P$ 为 $R_{\mathfrak{p}}$-模正合序列. 通过 $f:R\to R_{\mathfrak{p}}, a\mapsto a/1$ 可将N和P看作是 R-模. 而 $0\to N\to P$ 也为 R-模正合序列. 由假设M是平坦 R-模，于是 $0\to M\otimes_R N\xrightarrow{1\otimes\varphi} M\otimes_R P$ 为 R-模正合序列，然后在 $\mathfrak{p}$ 处局部化得到 $R_{\mathfrak{p}}$-模正合序列 $0\longrightarrow (M\otimes_R N)_{\mathfrak{p}}\xrightarrow{(1\otimes\varphi)_{\mathfrak{p}}}(M\otimes_R P)_{\mathfrak{p}}$. 容易验证图表

$$\begin{array}{ccccc} 0\longrightarrow & (M\otimes_R N)_{\mathfrak{p}} & \xrightarrow{(1\otimes\varphi)_{\mathfrak{p}}} & (M\otimes_R P)_{\mathfrak{p}} \\ & \lambda\uparrow & & \uparrow\mu \\ 0\longrightarrow & M_{\mathfrak{p}}\otimes_{R_{\mathfrak{p}}}N_{\mathfrak{p}} & \xrightarrow{1\otimes\varphi_{\mathfrak{p}}} & M_{\mathfrak{p}}\otimes_{R_{\mathfrak{p}}}P_{\mathfrak{p}} \end{array}$$

是交换的. 其中 λ 为标准 $R_{\mathfrak{p}}$-模同构，使得 $\lambda\left(\frac{m}{s}\otimes\frac{n}{t}\right)=\frac{m\otimes n}{st}$ $(m\in M, n\in N, s, t\in R-\mathfrak{p})$. μ 为类似定义的 $R_{\mathfrak{p}}$-模同构（定理4）. 由于N和P已经假定是 $R_{\mathfrak{p}}$-模. 从而 $N_{\mathfrak{p}}=N, P_{\mathfrak{p}}=P, \varphi_{\mathfrak{p}}=\varphi$. 由于 λ 和 μ 均是同构，从而由交换图表的上行正合性即得到下行正合性，也就是说 $0\longrightarrow M_{\mathfrak{p}}\otimes_{R_{\mathfrak{p}}}N\xrightarrow{1\otimes\varphi}M_{\mathfrak{p}}\otimes_{R_{\mathfrak{p}}}P$ 是 $R_{\mathfrak{p}}$-模正合序列. 这就表明 $M_{\mathfrak{p}}$是平坦 $R_{\mathfrak{p}}$-模.

(2)⇒(3)：显然.

(3)⇒(1)：设 $f:N\to P$ 是 R-模单同态，则对每个 $\mathfrak{m}\in \mathrm{Max}R$, $f_{\mathfrak{m}}:N_{\mathfrak{m}}\to P_{\mathfrak{m}}$是$R_{\mathfrak{m}}$-模单同态(引理 8). 从而由(3)推得$f_{\mathfrak{m}}\otimes 1:N_{\mathfrak{m}}\otimes_{R_{\mathfrak{m}}}M_{\mathfrak{m}}\to P_{\mathfrak{m}}\otimes_{R_{\mathfrak{m}}}M_{\mathfrak{m}}$为 $R_{\mathfrak{m}}$-模单同态(对每个$\mathfrak{m}\in \mathrm{Max}R$). 这相当于说 $(f\otimes 1)_{\mathfrak{m}}:(N\otimes_R M)_{\mathfrak{m}}\to (P\otimes_R M)_{\mathfrak{m}}$ 为 $R_{\mathfrak{m}}$ 模单同态. 于是由引理 8 可知 $N\otimes_R M\xrightarrow{f\otimes 1}P\otimes_R M$ 为 R-模单同态. 这就表明M是平坦 R-模. ▌

习　　题

1．设S为整环R的乘法集．M为R-模，$T(M)$为M的扭子模．求证：

(1) $T(S^{-1}M)=S^{-1}(T(M))$．

(2) M为无扭R-模$\Longleftrightarrow$对每个$\mathfrak{p}\in\mathrm{Spec}R$，$M_{\mathfrak{p}}$为无扭$R_{\mathfrak{p}}$-模$\Longleftrightarrow$对每个$\mathfrak{m}\in\mathrm{Max}R$，$M_{\mathfrak{m}}$为无扭$R_{\mathfrak{m}}$-模．

(3) M为扭R-模(即$M=T(M)$)$\Longleftrightarrow$对每个$\mathfrak{p}\in\mathrm{Spec}R$，$M_{\mathfrak{p}}$为扭$R_{\mathfrak{p}}$-模$\Longleftrightarrow$对每个$\mathfrak{m}\in\mathrm{Max}R$，$M_{\mathfrak{m}}$为扭$R_{\mathfrak{m}}$-模．

2．设M为R-模，$\mathfrak{a}$为R的理想．如果对每个包含$\mathfrak{a}$的极大理想$\mathfrak{m}$均有$M_{\mathfrak{m}}=0$，求证$M=\mathfrak{a}M$．

3．设R为整环，K为R的商域．

(1) 如果$a\in R$，$a\neq 0$并且$a\notin U(R)$，求证存在$\mathfrak{p}\in\mathrm{Spec}R$，使得$a^{-1}\notin R_{\mathfrak{p}}$．

(2) 求证 $\bigcap\limits_{\mathfrak{m}\in\mathrm{Max}R}R_{\mathfrak{m}}=\bigcap\limits_{\mathfrak{p}\in\mathrm{Spec}R}R_{\mathfrak{p}}=R$(注意：$R_{\mathfrak{p}}$均是$K$的子环)．

(3) 设$a,b\in R$，$ab\neq 0$．求证在R中$a|b\Longleftrightarrow$对每个$\mathfrak{p}\in\mathrm{Spec}R$，在$R_{\mathfrak{p}}$中$a|b\Longleftrightarrow$对每个$\mathfrak{m}\in\mathrm{Max}R$，在$R_{\mathfrak{m}}$中$a|b$．(注意：$R_{\mathfrak{p}}$均是整环．)

4．设$f:L\to M$和$g:M\to N$均是R-模同态．求证下列三条件彼此等价：

(1) $0\to L\xrightarrow{f}M\xrightarrow{g}N\longrightarrow 0$是$R$-模短正合序列．

(2) 对每个$\mathfrak{p}\in\mathrm{Spec}R$，$0\longrightarrow L_{\mathfrak{p}}\xrightarrow{f_{\mathfrak{p}}}M_{\mathfrak{p}}\xrightarrow{g_{\mathfrak{p}}}N_{\mathfrak{p}}\longrightarrow 0$均是$R_{\mathfrak{p}}$-模短正合序列．

(3) 对每个$\mathfrak{m}\in\mathrm{Max}R$，$0\longrightarrow L_{\mathfrak{m}}\xrightarrow{f_{\mathfrak{m}}}M_{\mathfrak{m}}\xrightarrow{g_{\mathfrak{m}}}N_{\mathfrak{m}}\longrightarrow 0$均是$R_{\mathfrak{m}}$-模短正合序列．

5．设R为整环，K为R的商域．M为有限生成投射R-模．求证

(1) $K\otimes_R M$是域K上有限维向量空间，并且对每个$\mathfrak{p}\in\mathrm{Spec}R$，$R_{\mathfrak{p}}$-模$M_{\mathfrak{p}}$均可自然地看成是$K\otimes_R M$的子集．

(2) $M=\bigcap\limits_{\mathfrak{p}\in\mathrm{Spec}R}M_{\mathfrak{p}}=\bigcap\limits_{\mathfrak{m}\in\mathrm{Max}R}M_{\mathfrak{m}}$．

6．设M是R-模．定义$\mathrm{Supp}(M)=\{\mathfrak{p}\in\mathrm{Spec}R\mid M_{\mathfrak{p}}\neq 0\}$．求证

(1) $M\neq 0 \Longleftrightarrow \mathrm{Supp}(M)\neq\varnothing$.

(2) 如果 $0\to M'\to M\to M''\to 0$ 是 R-模正合序列，则 $\mathrm{Supp}(M)=\mathrm{Supp}(M')\cup\mathrm{Supp}(M'')$.

(3) 如果M和N均是有限生成 R-模，则 $\mathrm{Supp}(M\otimes_R N)=\mathrm{Supp}(M)\cap\mathrm{Supp}(N)$.

第四章　Noether 环和 Artin 环

德国女数学家 E. Noether 于本世纪初对于理想准素分解特性的研究是传统理想论的支柱。这项工作使古典代数几何建立在全新的代数基础之上。在这一章里，我们首先介绍 Noether 的准素分解理论，然后讲具有理想准素分解特性的一类最重要的环——Noether 环以及 Noether 模。最后介绍在某种程度上与之对偶的 Artin 环以及 Artin 模。

§ 4.1　理想的准素分解

在整数环 Z 中，每个整数 $n\geqslant 2$ 均可唯一地表成一些素数之乘积：$n=p_1^{a_1}\cdots p_s^{a_s}$。但是任意(具有幺元素的交换)环 R 中没有这样好的性质。在某种程度上，素理想是素数的推广。我们可以把 n 的素数分解式写成理想的形式：

$$(n)=(p_1)^{a_1}\cap(p_2)^{a_2}\cap\cdots\cap(p_s)^{a_s}.$$

每个环中均有素理想概念，但不是每个理想均可表成有限个素理想之交(例如 Z 中的理想 4 Z)。Noether 发现，在相当广的一类环中有所谓准素分解特性，即每个理想均可写成有限个准素理想的交，并且这种表法还具有某种程度的唯一性。所谓准素理想可看作是整数环中"素数幂 p^a"的一种推广。它的确切含义是

定义　环 R 中的理想 $\mathfrak{q}$ 叫作是**准素**的，是指它满足如下两个条件：

(1) $\mathfrak{q}\neq R$;

(2) 如果 $x,y\in R$, $xy\in\mathfrak{q}$, $x\notin\mathfrak{q}$，则有正整数 n，使得 $y^n\in\mathfrak{q}$.

注记　条件(2)等价于以下诸条件：

(2′) 若 $xy\in\mathfrak{q}$, $x\notin\mathfrak{q}$，则 $y\in\sqrt{\mathfrak{q}}$.

(2″) 若 $xy\in\mathfrak{q}$, $y\notin\sqrt{\mathfrak{q}}$，则 $x\in\mathfrak{q}$.

$(2''')$ $R/\mathfrak{q}$ 中的零因子必为幂零元素(即 $R/\mathfrak{q}$ 的零因子属于 $R/\mathfrak{q}$ 的小根).

由定义不难看出:

例 1 环 R 中每个素理想必是准素理想(定义条件(2)中可取 $n=1$).

例 2 在整数环 $\mathbf{Z}$ 中,$n\mathbf{Z}$ 为准素理想$\Longleftrightarrow n=0$ 或者 $|n|=p^{\alpha}$(p 为素数,$\alpha\geqslant 1$). 对于任意主理想整环也有类似的命题.

例 3 设 $f: A\to B$ 为环的同态. 若 $\mathfrak{q}$ 为 B 的准素理想,则 $\mathfrak{q}^c=f^{-1}(\mathfrak{q})$ 为 A 的准素理想. (请读者自证)

引理 1 如果 $\mathfrak{q}$ 是环 R 的准素理想,则 $\sqrt{\mathfrak{q}}$ 为素理想,并且是包含 $\mathfrak{q}$ 的最小素理想.

证明 由于 $\sqrt{\mathfrak{q}}=\bigcap\limits_{\substack{\mathfrak{p}\in \mathrm{Spec}R\\ \mathfrak{p}\supseteq\mathfrak{q}}}\mathfrak{p}$,从而只需证明 $\sqrt{\mathfrak{q}}$ 为素理想即可.

设 $xy\in\sqrt{\mathfrak{q}}$,则有 $m\geqslant 1$ 使得 $x^m y^m=(xy)^m\in\mathfrak{q}$. 如果 $x^m\in\mathfrak{q}$,则 $x\in\sqrt{\mathfrak{q}}$. 如果 $x^m\notin\mathfrak{q}$,则又有 $n\geqslant 1$ 使得 $(y^m)^n=y^{mn}\in\mathfrak{q}$. 于是 $y\in\sqrt{\mathfrak{q}}$. 这就是说,x 和 y 至少有一个属于 $\sqrt{\mathfrak{q}}$. 从而 $\sqrt{\mathfrak{q}}$ 为素理想. ▌

定义 设 $\mathfrak{q}$ 为环 R 的准素理想. 我们把 $\mathfrak{p}=\sqrt{\mathfrak{q}}$ 叫作是**属于 $\mathfrak{q}$ 的素理想**,而 $\mathfrak{q}$ 叫作是 **$\mathfrak{p}$-准素理想**.

例 4 准素理想不一定是素理想的幂. 例如设 k 为域而 $R=k[x,y]$. 考虑 R 的理想 $\mathfrak{q}=(x,y^2)$,则 $R/\mathfrak{q}\cong k[y]/(y^2)\neq(0)$. 易知 $k[y]/(y^2)$ 中零因子必为幂零元素,从而 $\mathfrak{q}$ 为 R 的准素理想. 而 $\mathfrak{p}=\sqrt{\mathfrak{q}}=(x,y)$. 并且 $\mathfrak{p}^2\subset\mathfrak{q}\subset\mathfrak{p}$. 如果 $\mathfrak{q}=\mathfrak{p}'^n$,$\mathfrak{p}'\in\mathrm{Spec}R$,则 $\mathfrak{p}^2\subset\mathfrak{p}'^n\subset\mathfrak{p}$. 将此式诸项求根即得到 $\mathfrak{p}\subseteq\mathfrak{p}'\subseteq\mathfrak{p}$. 即 $\mathfrak{p}'=\mathfrak{p}$. 于是 $\mathfrak{p}^2\subset\mathfrak{p}^n\subset\mathfrak{p}$. 但这是不可能的. 从而 $\mathfrak{q}$ 不是素理想的幂.

例 5 素理想的幂也不一定是准素理想．例如设 k 为域而令 $R=k[x,y,z]/(xy-z^2)$．考查 R 的理想 $\mathfrak{p}=(\bar{x},\bar{z})$，则 $R/\mathfrak{p}\cong k[y]$ 为整环．从而 $\mathfrak{p}$ 为 R 的素理想．但是 $\mathfrak{p}^2$ 不是 R 的准素理想，因为 $\bar{x}\bar{y}=\bar{z}^2\in\mathfrak{p}^2$，$\bar{x}\notin\mathfrak{p}^2$ 而同时又有 $\bar{y}\notin\mathfrak{p}=\sqrt{\mathfrak{p}^2}$．

另一方面，我们有如下的引理．

引理 2 设 $\mathfrak{a}$ 为环 R 的理想．如果 $\sqrt{\mathfrak{a}}$ 是 R 的极大理想，则 $\mathfrak{a}$ 为准素理想．特别地，极大理想 $\mathfrak{m}$ 的方幂必是 $\mathfrak{m}$-准素理想．

证明 设 $\mathfrak{m}=\sqrt{\mathfrak{a}}\in\operatorname{Max}R$．则 $\mathfrak{m}$ 在 $R/\mathfrak{a}$ 中的象 $\bar{\mathfrak{m}}$ 是 $R/\mathfrak{a}$ 的小根．由于 R 中包含 $\mathfrak{a}$ 的素理想必然包含 $\mathfrak{m}=\sqrt{\mathfrak{a}}$，而 $\mathfrak{m}$ 又是 R 的极大理想．从而 $\mathfrak{m}$ 就是 R 中包含 $\mathfrak{a}$ 的唯一素理想．这表明 $R/\mathfrak{a}$ 为局部环．从而 $R/\mathfrak{a}$ 中零因子均属于 $\bar{\mathfrak{m}}$（因为零因子不是单位），由于 $\bar{\mathfrak{m}}$ 是 $R/\mathfrak{a}$ 的小根，从而 $R/\mathfrak{a}$ 中零因子均为幂零元素．于是 $\mathfrak{a}$ 为 R 的准素理想．引理 2 的最后一个论断是由于 $\sqrt{\mathfrak{m}^n}=\mathfrak{m}$．▌

引理 3 设 $\mathfrak{q}_i(1\leqslant i\leqslant n)$ 均为环 R 的理想，$\mathfrak{p}\in\operatorname{Spec}R$．如果每个 $\mathfrak{q}_i(1\leqslant i\leqslant n)$ 均是 $\mathfrak{p}$-准素理想，则 $\mathfrak{q}=\bigcap_{i=1}^{n}\mathfrak{q}_i$ 也是 $\mathfrak{p}$-准素理想．

证明 首先我们有 $\sqrt{\mathfrak{q}}=\sqrt{\bigcap\mathfrak{q}_i}=\bigcap\sqrt{\mathfrak{q}_i}=\mathfrak{p}$．其次，若 $xy\in\mathfrak{q}$，$y\notin\mathfrak{q}$，则有 $i(1\leqslant i\leqslant n)$ 使得 $xy\in\mathfrak{q}_i$，$y\notin\mathfrak{q}_i$．于是 $x\in\sqrt{\mathfrak{q}_i}=\mathfrak{p}=\sqrt{\mathfrak{q}}$．这就表明 $\mathfrak{q}$ 是 $\mathfrak{p}$-准素理想．▌

引理 4 设 $\mathfrak{q}$ 是环 R 的 $\mathfrak{p}$-准素理想，$x\in R$．则

(1) $x\in\mathfrak{q}\Rightarrow(\mathfrak{q}:x)=R$．

(2) $x\notin\mathfrak{p}\Rightarrow(\mathfrak{q}:x)=\mathfrak{q}$．

(3) $x\notin\mathfrak{q}\Rightarrow(\mathfrak{q}:x)$ 为 $\mathfrak{p}$-准素理想．

证明 (1)和(2)由定义直接得出．对于(3)，我们先求 $\sqrt{(\mathfrak{q}:x)}$：若 $y\in(\mathfrak{q}:x)$，则 $xy\in\mathfrak{q}$．但是 $x\notin\mathfrak{q}$，于是 $y\in\mathfrak{p}$．这表

明$\mathfrak{q}\subseteq(\mathfrak{q}:x)\subseteq\mathfrak{p}$. 取根，即知$\mathfrak{p}\subseteq\sqrt{(\mathfrak{q}:x)}\subseteq\mathfrak{p}$. 因此$\sqrt{(\mathfrak{q}:x)}=\mathfrak{p}$. 再证$(\mathfrak{q}:x)$准素：若 $yz\in(\mathfrak{q}:x)$, $y\notin\mathfrak{p}(=\sqrt{(\mathfrak{q}:x)})$，则 $xyz\in\mathfrak{q}$. 但是 $y\notin\mathfrak{p}$，而 $\mathfrak{q}$ 为 $\mathfrak{p}$-准素理想，从而 $xz\in\mathfrak{q}$. 于是 $z\in(\mathfrak{q}:x)$. 这就表明$(\mathfrak{q}:x)$是$\mathfrak{p}$-准素理想. ▌

定义 环R的理想 $\mathfrak{a}$ 叫作是**可分解的**，是指 $\mathfrak{a}$ 可表示成有限个准素理想之交，即

$$\mathfrak{a}=\bigcap_{i=1}^{n}\mathfrak{q}_i \qquad (\mathfrak{q}_i\text{均准素}). \tag{1}$$

这时，我们称(1)式为理想 $\mathfrak{a}$ 的**准素分解式**. 每个 $\mathfrak{q}_i$ 叫作是 $\mathfrak{a}$ 的**准素分支**.

一般说来，不是每个理想都是可分解的. 我们在下节要证明，对于代数几何中很重要的一类环——Noether 环，其中每个理想均是可分解的，即均有准素分解式. 在本节中，我们先假定理想 $\mathfrak{a}$ 是可分解的，考查准素分解式的唯一性问题，即准素分解式中哪些因素是由理想 $\mathfrak{a}$ 所唯一决定的.

首先，如果准素分解式(1)中某个准素分支 $\mathfrak{q}_j$ 包含其余 $n-1$ 个准素分支的交，那末(1)式中显然可以去掉这个 $\mathfrak{q}_j$，得到 $\mathfrak{a}$ 的一个更简单的准素分解式. 其次，如果准素分支中某一些有相同的根. 例如$\sqrt{\mathfrak{q}_1}=\cdots=\sqrt{\mathfrak{q}_r}=\mathfrak{p}$. 由引理 3 我们知道 $\mathfrak{q}=\bigcap_{i=1}^{r}\mathfrak{q}_i$ 仍是 $\mathfrak{p}$-准素理想. 于是，将(1)式中 $\bigcap_{i=1}^{r}\mathfrak{q}_i$ 改成一个 $\mathfrak{q}$，又得到一个更简单的准素分解式. 所以，若理想 $\mathfrak{a}$ 是可分解的，我们总可经过上述“简化”得到形如(1)的准素分解式，使得它还满足如下两个条件：

(a) $\sqrt{\mathfrak{q}_i}\,(1\leqslant i\leqslant n)$是彼此不同的素理想；

(b) $\mathfrak{q}_j \not\supseteq \bigcap_{\substack{i=1 \\ i \neq j}}^{n} \mathfrak{q}_i \qquad (1 \leqslant j \leqslant n)$.

定义 满足条件(a)和(b)的准素分解式(1)叫作是理想 $\mathfrak{a}$ 的**极小准素分解式**.

然而,理想 $\mathfrak{a}$ 的极小准素分解式(如果有的话)也仍然有可能不是唯一的.

例 6 $R=k[x,y]$(k 为域). 理想 $\mathfrak{a}=(x^2,xy)$有如下两个不同的极小准素分解式:

$\mathfrak{a}=(x)\cap(x,y)^2 \qquad$ ($(x,y)^2$ 是极大理想(x,y)的幂, 从而准素).

$\mathfrak{a}=(x)\cap(x^2,y) \qquad$ ((x^2,y) 的准素性见例 4).

注意$\sqrt{(x)}=(x)$, $\sqrt{(x,y)^2}=\sqrt{(x^2,y)}=(x,y)$. 从而这两个均是极小准素分解式.

下面定理表明准素分解式在某种程度上的唯一性.

定理 1 (第一唯一性定理)设 $\mathfrak{a}=\bigcap_{i=1}^{n}\mathfrak{q}_i$ 是极小准素分解式. $\mathfrak{p}_i=\sqrt{\mathfrak{q}_i}\,(1\leqslant i\leqslant n)$. 则$\{\mathfrak{p}_1,\cdots,\mathfrak{p}_n\}$是由 $\mathfrak{a}$ 所决定的, 与极小准素分解式无关.

证明 我们来证明

$\{\mathfrak{p}_1,\cdots,\mathfrak{p}_n\}=\{\mathfrak{p}\in \operatorname{Spec} R \mid$ 存在 $x\in R$ 使得 $\mathfrak{p}=\sqrt{(\mathfrak{a}:x)}\}$.

由于此式右边完全是理想 $\mathfrak{a}$ 本身的特性,由此即可证得定理 1.

对于每个 $x\in R$, $(\mathfrak{a}:x)=\left(\bigcap_{i=1}^{n}\mathfrak{q}_i:x\right)=\bigcap_{i=1}^{n}(\mathfrak{q}_i:x)$. 于是由引理 4 的(1)和(3)可知

$$\sqrt{(\mathfrak{a}:x)}=\bigcap_{i=1}^{n}\sqrt{(\mathfrak{q}_i:x)}=\bigcap_{\substack{j=1 \\ x\notin \mathfrak{q}_j}}^{n}\mathfrak{p}_j. \tag{2}$$

如果$\sqrt{(\mathfrak{a}:x)}$为素理想，则由(2)式可知存在某个 j 使得$\sqrt{(\mathfrak{a}:x)}=\mathfrak{p}_j$. 反之，由准素分解式的极小性可知对每个 j 都有 $x_j\in R$ 使得 $x_j\notin\mathfrak{q}_j$, $x_j\in\bigcap_{\substack{i=1\\i\neq j}}^{n}\mathfrak{q}_i$. 于是由(2)式可知 $\sqrt{(\mathfrak{a}:x_j)}=\mathfrak{p}_j$. 这就完成了证明. ▌

注记 由上述证明和引理 4，可知对每个 $j(1\leqslant j\leqslant n)$，均有 $x_j\in R$，使得$(\mathfrak{a}:x_j)$为 $\mathfrak{p}_j$-准素理想.

定义 定理 1 中每个 $\mathfrak{p}_j(1\leqslant j\leqslant n)$ 均叫作是**属于 $\mathfrak{a}$ 的素理想**.

于是，当 $\mathfrak{a}$ 是可分解理想时，$\mathfrak{a}$ 为准素理想的充要条件是 $\mathfrak{a}$ 只有一个属于它的素理想.

例 6 中理想 $\mathfrak{a}=(x^2,xy)$的两个不同的极小准素分解式具有同样的$\{\mathfrak{p}_1,\mathfrak{p}_2\}=\{(x),(x,y)\}$. 注意$(x)\subseteq(x,y)$. 从而$\sqrt{\mathfrak{a}}=\mathfrak{p}_1\cap\mathfrak{p}_2=(x)$为素理想，但 $\mathfrak{a}$ 不是准素理想. 这说明 $\mathfrak{a}$ 的根为素理想则 $\mathfrak{a}$ 不必准素(例 5 也是这方面的例子). 例 6 还启发我们给出如下的定义：

定义 设理想 $\mathfrak{a}$ 有极小准素分解式：$\mathfrak{a}=\bigcap_{i=1}^{n}\mathfrak{q}_i$，$\mathfrak{p}_i=\sqrt{\mathfrak{q}_i}$. 则$\{\mathfrak{p}_1,\cdots,\mathfrak{p}_n\}$中每个极小元叫作是属于$\mathfrak{a}$ 的**极小素理想**或**孤立素理想**. 如果 $\mathfrak{p}_i$ 是孤立素理想，则对应的 $\mathfrak{q}_i$ 叫作是 $\mathfrak{a}$ 的**孤立准素分支**. 不是孤立素理想的 $\mathfrak{p}_i$ 叫作是属于 $\mathfrak{a}$ 的**嵌入素理想**，对应的 $\mathfrak{q}_i$ 叫作是 $\mathfrak{a}$ 的**嵌入准素分支**. (“孤立”和“嵌入”二词起源于它所反映的代数几何事实. 见 §6.1 中的解释).

比如在例 6 中，(x)和(x,y)分别是属于 $\mathfrak{a}=(x^2,xy)$ 的极小(孤立)素理想和嵌入素理想.

由于$\{\mathfrak{p}_1,\cdots,\mathfrak{p}_n\}$是由$\mathfrak{a}$所决定，而其中的全部极小元，即属于

$\mathfrak{a}$ 的全部极小素理想当然也是由 $\mathfrak{a}$ 所决定的. 事实上我们可以把它们刻画成

引理 5 设 $\mathfrak{a}$ 是可分解理想,则每个包含 $\mathfrak{a}$ 的素理想必包含某个属于 $\mathfrak{a}$ 的极小素理想. 于是属于 $\mathfrak{a}$ 的全部极小素理想恰好就是集合 $\{\mathfrak{p}\in \mathrm{Spec}\, R \mid \mathfrak{p}\supseteq\mathfrak{a}\}$ 的全部极小元.

证明 如果 $\mathfrak{p}\supseteq\mathfrak{a}=\bigcap\limits_{i=1}^{n}\mathfrak{q}_i$. 取根则有 $\mathfrak{p}\supseteq\bigcap\limits_{i=1}^{n}\mathfrak{p}_i=$ 属于 $\mathfrak{a}$ 的全部极小素理想之交. 从而 $\mathfrak{p}$ 必然包含某个属于 $\mathfrak{a}$ 的极小素理想. 由此易得到引理 5 的后一个论断. ▌

引理 6 (1) 设 $\mathfrak{a}=\bigcap\limits_{i=1}^{n}\mathfrak{q}_i$ 是理想 $\mathfrak{a}$ 的极小准素分解式, $\mathfrak{p}_i=\sqrt{\mathfrak{q}_i}$. 则

$$\bigcup_{i=1}^{n}\mathfrak{p}_i=\{x\in R \mid (\mathfrak{a}:x)\supset\mathfrak{a}\}.$$

(2) 若零理想(0)是可分解的,则 R 的零因子集合 D 为属于(0)的全部素理想之并.

证明 (1) 不难证明: $\mathfrak{a}=\bigcap\limits_{i=1}^{n}\mathfrak{q}_i$ 是 $\mathfrak{a}$ 在 R 中极小准素分解式 $\Longleftrightarrow(\overline{0})=\bigcap\limits_{i=1}^{n}\bar{\mathfrak{q}}_i$ 是 $(\overline{0})$ 在 $R/\mathfrak{a}$ 中的极小准素分解式. 从而由 $R/\mathfrak{a}$ 中素理想和 R 的包含 $\mathfrak{a}$ 的素理想之间的保序一一对应关系,可知由(2)可推出(1). 为了证明(2)式,我们由 D 的定义知道 $D=\bigcup\limits_{\substack{x\in R\\ x\neq 0}}(0:x)$. 由此式还可得到 D 的另一表达式:

$$D=\bigcup_{\substack{x\in R\\ x\neq 0}}\sqrt{(0:x)}. \tag{3}$$

这是因为D显然包含在(3)式右边之中.反之,如果y属于(3)式右边,则有$x\neq 0$,使得$y\in\sqrt{(0:x)}$.于是有$n\geqslant 1$,使得$y^n\in(0:x)$.从而$y^nx=0$.由于$x\neq 0$,于是有正整数i使得$y^ix=y(y^{i-1}x)=0$,而$y^{i-1}x\neq 0$.从而$y\in(0:y^{i-1}x)$,即$y\in D$.因此等式(3)成立.

设$(0)=\bigcap_{i=1}^{n}\mathfrak{q}_i$为极小准素分解式,$\mathfrak{p}_i=\sqrt{\mathfrak{q}_i}$.由定理1的证明中的(2)式可知

$$\sqrt{(0:x)}=\bigcap_{x\notin\mathfrak{q}_j}\mathfrak{p}_j. \tag{4}$$

如果$x\neq 0$,则$1\notin(0:x)$.从而$(0:x)\neq R$,于是$\sqrt{(0:x)}\neq R$.由(4)式可知有$j(1\leqslant j\leqslant n)$使得$\sqrt{(0:x)}\subset\mathfrak{p}_j$.再由(3)式即知$D\subseteq\bigcup_{i=1}^{n}\mathfrak{p}_i$.反之,由定理1的证明可知每个$\mathfrak{p}_i$均有形式$\mathfrak{p}_i=\sqrt{(0:x)}$(对某个$0\neq x\in R$).因此又有$\bigcup_{i=1}^{n}\mathfrak{p}_i\subseteq\bigcup_{\substack{x\in R\\x\neq 0}}\sqrt{(0:x)}=D$. ▌

注记 当(0)可分解时,引理6表明R的零因子集合为属于(0)的所有素理想之**并**,而R的幂零元集合(即R的小根$\sqrt{(0)}$)则为属于(0)的所有素理想之**交**.

例如对于$R=\mathbf{Z}/12\mathbf{Z}$,$(0)=(\overline{3})\cap(\overline{4})$是零理想的准素分解式.属于(0)的两个素理想是$(\overline{3})$和$(\overline{2})$.于是环$R$的零因子集合为$(\overline{3})\cup(\overline{2})=\{\overline{0},\overline{3},\overline{6},\overline{9},\overline{2},\overline{4},\overline{8},\overline{10}\}$.而幂零元集合为$(\overline{3})\cap(\overline{2})=\{\overline{0},\overline{6}\}$.

现在谈局部化过程中准素理想的性状.

定理 2 设S为环R的乘法集,$\mathfrak{q}$为R中的$\mathfrak{p}$-准素理想.

(1) 若 $S\cap\mathfrak{p}\neq\varnothing$，则 $S^{-1}\mathfrak{q}=S^{-1}R$.

(2) 若 $S\cap\mathfrak{p}=\varnothing$，则 $S^{-1}\mathfrak{q}$ 是$S^{-1}R$ 中的 $S^{-1}\mathfrak{p}$-准素理想，并且$(S^{-1}\mathfrak{q})^c=\mathfrak{q}$.

(3) 在理想的扩张映射和限制映射之下，集合 $C=\{R$ 中准素理想 $\mathfrak{q}\mid\sqrt{\mathfrak{q}}\cap S=\varnothing\}$和集合$E=\{S^{-1}R$中准素理想$\}$之间是保序一一对应的.

证明 (1) 令 $s\in S\cap\mathfrak{p}$，则有 $n\geqslant1$ 使得 $s^n\in S\cap\mathfrak{q}$. 于是$\frac{s^n}{1}\in S^{-1}\mathfrak{q}$ 并且$\frac{1}{s^n}\in S^{-1}R$，从而$\frac{1}{1}=\frac{s^n}{1}\cdot\frac{1}{s^n}\in S^{-1}\mathfrak{q}$，即 $S^{-1}\mathfrak{q}=S^{-1}R$.

(2) 如果 $S\cap\mathfrak{p}=\varnothing$，则由 $s\in S$，$as\in\mathfrak{q}$ 可推出 $a\in\mathfrak{q}$(这是因为 $s\notin\mathfrak{p}$). 根据第三章定理1，可知 $\mathfrak{q}^{ec}=\bigcup\limits_{s\in S}(\mathfrak{q}:s)=\mathfrak{q}$. 进而，$\sqrt{\mathfrak{q}^e}=\sqrt{S^{-1}\mathfrak{q}}=S^{-1}\sqrt{\mathfrak{q}}=S^{-1}\mathfrak{p}$，这是 $S^{-1}R$ 中的素理想. 然后证明 $S^{-1}\mathfrak{q}$ 为 $S^{-1}\mathfrak{p}$-准素理想即可$\left(\frac{a}{s_1}\cdot\frac{b}{s_2}\in S^{-1}\mathfrak{q},\ \frac{a}{s_1}\notin S^{-1}\mathfrak{q}\Rightarrow ab\in\mathfrak{q},\ a\notin\mathfrak{q}\Rightarrow b\in\mathfrak{p}\Rightarrow\frac{b}{s_2}\in S^{-1}\mathfrak{p}\right)$.

(3) 注意到 $S^{-1}R$ 中理想均可表示成形式 $S^{-1}\mathfrak{a}$，其中 $\mathfrak{a}$ 为R中理想，则由(1)和(2)即可证得(3). ▌

定理 3 设S为环R的乘法集. $\mathfrak{a}=\bigcap\limits_{i=1}^{n}\mathfrak{q}_i$ 为理想 $\mathfrak{a}$ 的极小准素分解式，$\mathfrak{p}_i=\sqrt{\mathfrak{q}_i}$. 又设

$$S\cap\mathfrak{p}_i=\varnothing(1\leqslant i\leqslant m),S\cap\mathfrak{p}_i\neq\varnothing(m+1\leqslant i\leqslant n).$$

则

(1) $S^{-1}\mathfrak{a}=\bigcap\limits_{i=1}^{m}S^{-1}\mathfrak{q}_i$ 是 $S^{-1}\mathfrak{a}$ 的极小准素分解式.

(2) $\mathfrak{a}^{ec}=(S^{-1}\mathfrak{a})^c=\bigcap_{i=1}^{m}\mathfrak{q}_i$ 是 $\mathfrak{a}^{ec}$ 的极小准素分解式.

证明 由定理 2 可知 $S^{-1}\mathfrak{a}=\bigcap_{i=1}^{n}S^{-1}\mathfrak{q}_i=\bigcap_{i=1}^{m}S^{-1}\mathfrak{q}_i$,并且 $S^{-1}\mathfrak{q}_i$ 是 $S^{-1}\mathfrak{p}_i$-准素理想. 由于 $\mathfrak{p}_i$ $(1\leqslant i\leqslant m)$ 两两不同, 从而 $S^{-1}\mathfrak{p}_i$ $(1\leqslant i\leqslant m)$ 也两两不同. 再由定理 2 中所述集合 C 与 E 之间的保序一一对应,即可知 $\bigcap_{i=1}^{m}S^{-1}\mathfrak{q}_i$ 是 $S^{-1}\mathfrak{a}$ 的极小准素分解式. 由(1)得到 $\mathfrak{a}^{ec}=\bigcap_{i=1}^{m}(S^{-1}\mathfrak{q}_i)^c=\bigcap_{i=1}^{m}\mathfrak{q}_i$. 这显然是极小准素分解式. ▌

注记 这是一条很有用的定理. 形象地说, 选取适当的乘法集 S,从 $\mathfrak{a}$ 到 $\mathfrak{a}^{ec}$, 我们可以"杀掉" $\mathfrak{a}$ 的一部分准素分支. 下面是这种原则的一个应用.

定义 设 $\mathfrak{a}$ 是可分解理想. 属于 $\mathfrak{a}$ 的一部分素理想组成的集合 Σ 叫作是**孤立集合**,是指:如果 $\mathfrak{p}'$ 是属于 $\mathfrak{a}$ 的素理想并且 $\mathfrak{p}'\subseteq\mathfrak{p}\in\Sigma$,则 $\mathfrak{p}'\in\Sigma$.

例如: 若 $\mathfrak{p}_1,\cdots,\mathfrak{p}_t$ 均是属于 $\mathfrak{a}$ 的孤立素理想, 则 $\Sigma=\{\mathfrak{p}_1,\cdots,\mathfrak{p}_t\}$就是一个孤立集合.

设 Σ 是属于 $\mathfrak{a}$ 的一个素理想孤立集合, 则 $S=R-\bigcup_{\mathfrak{p}\in\Sigma}\mathfrak{p}$ 是 R 的乘法集, 并且对于属于 $\mathfrak{a}$ 的每个素理想 $\mathfrak{p}'$,如果 $\mathfrak{p}'\in\Sigma$,必然 $\mathfrak{p}'\cap S=\varnothing$;反之若 $\mathfrak{p}'\cap S=\varnothing$, 则 $\mathfrak{p}'\subseteq\bigcup_{\mathfrak{p}\in\Sigma}\mathfrak{p}$. 从而存在 $\mathfrak{p}\in\Sigma$ 使得 $\mathfrak{p}'\subseteq\mathfrak{p}$. 由于 Σ 是孤立集合, 因此 $\mathfrak{p}'=\mathfrak{p}\in\Sigma$. 这些事实可用来证明

定理 4（第二唯一性定理） 设 $\mathfrak{a}=\bigcap_{i=1}^{n}\mathfrak{q}_i$ 为极小准素分解式，$\mathfrak{p}_i=\sqrt{\mathfrak{q}_i}$. $\Sigma=\{\mathfrak{p}_{i_1},\cdots,\mathfrak{p}_{i_m}\}$是属于 $\mathfrak{a}$ 的一个素理想孤立集合，则 $\bigcap_{k=1}^{m}\mathfrak{q}_{i_k}$ 是由 $\mathfrak{a}$ 和 Σ 所决定的，与极小准素分解式无关.

证明 取 $S=R-(\mathfrak{p}_{i_1}\cup\cdots\cup\mathfrak{p}_{i_m})$. 由定理 4 前面所述的事实和定理 3，可知 $\mathfrak{a}^{ec}=(S^{-1}\mathfrak{a})^c=\mathfrak{q}_{i_1}\cap\cdots\cap\mathfrak{q}_{i_m}$. 由于 S^{-1}只依赖于Σ，从而 $\bigcap_{k=1}^{m}\mathfrak{q}_{i_k}$ 只依赖于 $\mathfrak{a}$ 和 Σ. ▌

系 设 $\mathfrak{p}_i$ 为属于 $\mathfrak{a}$ 的孤立素理想，则它所对应的孤立准素分支 $\mathfrak{q}_i$ 是由 $\mathfrak{a}$ 和 $\mathfrak{p}_i$ 所决定的. 特别地，每个可分解理想 $\mathfrak{a}$ 的全体孤立准素分支所组成的集合是由 $\mathfrak{a}$ 所唯一决定的.

证明 在定理 4 中取 $\Sigma=\{\mathfrak{p}_i\}$即可. ▌

例如在前面的例 6 中，理想 (x^2,xy) 有两个不同的极小准素分解式：$(x)\cap(x,y)^2$ 和 $(x)\cap(x^2,y)$. 其中嵌入准素分支可以不同：$(x,y)^2\neq(x^2,y)$. 但是孤立准素分支均为(x).

习　题

1. 在多项式环 $\mathbf{Z}[x]$中，$\mathfrak{m}=(2,x)$是极大理想，$\mathfrak{q}=(4,x)$为 $\mathfrak{m}$-准素理想，但 $\mathfrak{q}$ 不是素理想的幂.

2. 设 k 为域，$R=k[x,y,z]$. 求证

(1) $\mathfrak{p}_1=(x,y)$ 和 $\mathfrak{p}_2=(x,z)$均为R的素理想，$\mathfrak{m}=(x,y,z)$ 是R的极大理想.

(2) 令 $\mathfrak{a}=\mathfrak{p}_1\mathfrak{p}_2$. 则 $\mathfrak{a}=\mathfrak{p}_1\cap\mathfrak{p}_2\cap\mathfrak{m}^2$ 为理想 $\mathfrak{a}$ 的极小准素分解式. 试问属于 $\mathfrak{a}$ 的极小素理想和嵌入素理想都有哪些?

3. (1) 令 $R=\mathbf{Z}[x,y]$. 求证对所有 $i,j\geqslant1$，(x^i,y^j)是 (x,y)- 准素理想.

(2) 给出R中理想 $\mathfrak{a}=(x^2,xy,2)$ 的一个极小准素分解式. 并求出属于

$\mathfrak{a}$ 的全部素理想. 由此决定$\sqrt{\mathfrak{a}}$.

4. 设 k 为域. 给出环 $k[x,y]$中理想(x^2,xy)的三个不同的极小准素分解式.

5. 设 $\mathfrak{a}$ 为环 R 的可分解理想. 如果 $\mathfrak{a}=\sqrt{\mathfrak{a}}$, 则属于 $\mathfrak{a}$ 的每个素理想均是孤立的.

6. 设 $\mathfrak{a}$ 为环 R 的理想,$\mathfrak{a}[x]=\{a_0+a_1x+\cdots+a_nx^n \mid a_i\in\mathfrak{a}\}$. 求证:

(1) $\mathfrak{a}[x]$ 是 $\mathfrak{a}$ 到环 $R[x]$ 中的扩张理想 (对于环同态 $f:R\to R[x]$, $a\mapsto a$).

(2) $\mathfrak{p}\in\mathrm{Spec}\ R\Rightarrow\mathfrak{p}[x]\in\mathrm{Spec}\ R[x]$.

(3) $\mathfrak{q}$ 为 R 中的 $\mathfrak{p}$-准素理想$\Rightarrow\mathfrak{q}[x]$为 $R[x]$ 中的 $\mathfrak{p}[x]$-准素理想. [提示: 利用 §1.3 习题 9.]

(4) $\mathfrak{a}=\bigcap\limits_{i=1}^{n}\mathfrak{q}_i$ 为 R 中的极小准素分解式$\Rightarrow\mathfrak{a}[x]=\bigcap\limits_{i=1}^{n}\mathfrak{q}_i[x]$为 $R[x]$ 中的极小准素分解式.

(5) $\mathfrak{p}$ 为属于 $\mathfrak{a}$ 的极小素理想$\Rightarrow\mathfrak{p}[x]$为属于 $\mathfrak{a}[x]$的极小素理想.

7. 设 k 为域,$R=k[x_1,\cdots,x_n]$.则对于每个$i(1\leqslant i\leqslant n)$,$\mathfrak{p}_i=(x_1,\cdots,x_i)$均是$R$的素理想,并且 $\mathfrak{p}_i$ 的幂均是R的准素理想. [提示: 利用习题 6.]

8. 设R为环,对 $a\in R$,令$P(a)=\{\mathfrak{p}\in\mathrm{Spec}R\mid\mathfrak{p}\supseteq(0:a)\}$,$D(R)=\{\mathfrak{p}\in\mathrm{Spec}\ R\mid$存在 $a\in R$ 使得 $\mathfrak{p}$ 为集合 $P(a)$的极小元$\}$. 求证: x 为R的零因子$\Longleftrightarrow$存在 $\mathfrak{p}\in D(R)$使得 $x\in\mathfrak{p}$.

9. 设S是环R的乘法集. 对于 $\mathfrak{p}\in\mathrm{Spec}R$,$\mathfrak{p}\cap S=\varnothing$, 将$\mathfrak{p}$ 等同于 $S^{-1}\mathfrak{p}\in\mathrm{Spec}(S^{-1}R)$. 由此将 $\mathrm{Spec}\ (S^{-1}R)$ 看成是 $\mathrm{Spec}\ R$ 的子集 (参见 §3.1 定理1(6)). 求证

(1) $D(S^{-1}R)=D(R)\cap\mathrm{Spec}(S^{-1}R)$($D(R)$的定义见习题 8).

(2) 如果R中零理想(0)是可分解的,则 $D(R)$ 恰好是属于(0)的素理想全体.

10. 对于 $\mathfrak{p}\in\mathrm{Spec}R$,以 $S_{\mathfrak{p}}(0)$表示同态 $f:R\to R_{\mathfrak{p}},a\mapsto a/1$ 的核. 求证:

(1) $S_{\mathfrak{p}}(0)\subseteq\mathfrak{p}$.

(2) $\sqrt{S_{\mathfrak{p}}(0)}=\mathfrak{p}\Longleftrightarrow\mathfrak{p}$ 是环 R 的极小素理想.

(3) $\mathfrak{p},\mathfrak{p}'\in\mathrm{Spec}R,\mathfrak{p}\supseteq\mathfrak{p}'\Rightarrow S_{\mathfrak{p}}(0)\subseteq S_{\mathfrak{p}'}(0)$.

(4) $\mathfrak{p}\bigcap\limits_{\in D} S_{\mathfrak{p}}(0)=(0)$，其中 $D(R)$ 的定义见习题 8.

(5) 如果 $\mathfrak{p}$ 为 R 的极小素理想，则 $S\mathfrak{p}(0)$ 是最小的 $\mathfrak{p}$-准素理想。

(6) 令 $\mathfrak{a}=\bigcap\limits_{\mathfrak{p}} S\mathfrak{p}(0)$，其中 $\mathfrak{p}$ 过 R 的全部极小素理想. 求证 $\mathfrak{a}\subseteq N(R)$（$R$ 的小根）。

(7) 设 R 的零理想 (0) 是可分解的. 求证：(6) 中定义的理想 $\mathfrak{a}=(0)\Longleftrightarrow$ 属于 (0) 的每个素理想均是孤立的。

11. 设 S 是环 R 的乘法集. 对于 R 的理想 $\mathfrak{a}$，令 $S(\mathfrak{a})=\mathfrak{a}^{ec}=(S^{-1}\mathfrak{a})^c$，叫作是 $\mathfrak{a}$ 对于 S 的**饱和化**. 求证：

(1) $S(\mathfrak{a})\cap S(\mathfrak{b})=S(\mathfrak{a}\cap\mathfrak{b})$。

(2) $S(N(\mathfrak{a}))=N(S(\mathfrak{a}))$。

(3) $S(\mathfrak{a})=R\Longleftrightarrow\mathfrak{a}\cap S\neq\varnothing$。

(4) 设 S_1,S_2 均为 R 的乘法集，则 $S_1(S_2(\mathfrak{a}))=(S_1S_2)(\mathfrak{a})$，其中 $S_1S_2=\{s_1s_2\mid s_1\in S_1, s_2\in S_2\}$。

(5) 如果理想 $\mathfrak{a}$ 是可分解的，求证集合 $\{S(\mathfrak{a})\mid S$ 为 R 的乘法集$\}$ 是有限集合。

12. 设 $\mathfrak{p}\in\mathrm{Spec}\,R$，$S=R-\mathfrak{p}$。定义 $\mathfrak{p}^{(n)}=S(\mathfrak{p}^n)$（右边记号见 11 题）。求证：

(1) $\mathfrak{p}^{(n)}$ 为 $\mathfrak{p}$-准素理想。

(2) 若 $\mathfrak{p}^n$ 可分解，则 $\mathfrak{p}^{(n)}$ 是 $\mathfrak{p}^n$ 的 $\mathfrak{p}$-准素分支。

(3) 若 $\mathfrak{p}^{(m)}\mathfrak{p}^{(n)}$ 是可分解理想，则 $\mathfrak{p}^{(m+n)}$ 是它的 $\mathfrak{p}$-准素分支。

(4) $\mathfrak{p}^{(n)}=\mathfrak{p}^n\Longleftrightarrow\mathfrak{p}^n$ 是 $\mathfrak{p}$-准素理想。

13. 设环 R 中理想 $\mathfrak{a}$ 是可分解的，$\mathfrak{p}$ 为理想集合 $\{(\mathfrak{a}:x)\mid x\in R-\mathfrak{a}\}$ 中的极大元. 求证 $\mathfrak{p}$ 是属于 $\mathfrak{a}$ 的素理想。

14. 设 S 为环 R 的乘法集. 如果 R 中每个理想均可分解，则环 $S^{-1}R$ 中每个理想也均可分解。

§ 4.2 Noether 模和 Noether 环

我们在上节讲述了理想准素分解的一些特性. 现在我们来介绍 Noether环. 在这类环中，每个理想均是可分解的，从而上节的全部结果对于这类环中的理想都适用. 我们从更一般的情形——

Noether 模谈起.

定义 R-模 M 叫作是 Noether 模，是指 M 的每个 R-子模都是有限生成的.

下面是它的几个等价条件.

定理 5 以 Σ 表示 R-模 M 的全部 R-子模所组成的集合，则下列三条件彼此等价：

(1) M 是 Noether R-模；

(2) (升链条件) Σ 中的升链都是稳定的，也就是说，如果

$$N_1\subseteq N_2\subseteq\cdots\subseteq N_n\subseteq\cdots \tag{I}$$

是 M 的子模升链，则存在 n_0，使得 $N_{n_0}=N_{n_0+1}=\cdots$

(3) (极大条件) Σ 的每个非空子集(对于包含关系)均有极大元.

证明 (1)⇒(2)：对于子模升链(I)，易证 $N=\bigcup_{n=1}^{\infty}N_n$ 也是 M 的子模，从而应当是有限生成的. 设 $N=Rx_1+\cdots+Rx_s$，则 $x_i\in N=\bigcup_{n=1}^{\infty}N_n$. 从而有 p_i 使得 $x_i\in N_{p_i}$ $(1\leqslant i\leqslant s)$. 取 $n_0=\mathrm{Max}\{p_1,\cdots,p_s\}$，则 $x_i\in N_{n_0}(1\leqslant i\leqslant s)$. 于是 $N\subseteq N_{n_0}\subseteq N_{n_0+1}\subseteq\cdots\subseteq N$. 从而 $N_{n_0}=N_{n_0+1}=\cdots$.

(2)⇒(3)：用反证法. 如果Σ的非空子集合 Σ' 没有极大元，则对于 $N_1\in\Sigma'$，必有 $N_2\in\Sigma'$使得 $N_1\subset N_2$. 类似地又有 $N_3\in\Sigma'$ 使得 $N_2\subset N_3$. 如此继续下去，我们就构作出一个不稳定的子模严格升链 $N_1\subset N_2\subset N_3\subset\cdots\subset N_n\subset\cdots$. 这与升链条件相矛盾.

(3)⇒(1)：设 P 是 M 的子模，定义集合

$$\Sigma'=\{P\text{ 的子模 }N\mid N\text{ 是有限生成 }R\text{-模}\}.$$

则 Σ'非空(因为$(0)\in\Sigma'$). 于是 Σ' 有极大元 N. 如果 $N\subset P$，

则有 $x\in P-N$. 那末 $N'=N+Rx$ 也是有限生成 R-模，并且为 P 的子模，从而 $N'\in\Sigma'$. 但是显然 $N'\supset N$，这就与 N 的极大性矛盾. 所以 $N=P$. 即 P 是有限生成 R-模. 这就表明 M 的每个子模都是有限生成的，即 M 是 Noether R-模. ▌

现在我们举一些例子

例 1 有限生成 Abel 群是 Noether $\mathbf{Z}$-模. 更一般地，由第二章所讲的主理想整环上有限生成模的结构定理不难看出，主理想整环 R 上的模 M 是 Noether 模 $\Longleftrightarrow M$ 是有限生成 R-模. 特别地，每个主理想整环 R 均是 Noether R-模.

注记 对于任意的环 R，有限生成 R-模 M 不一定是Noether 模. 因为 M 的子模不一定有限生成. 例如取 $R=k[x_1,\cdots,x_n,\cdots]$（域 k 上无穷多个文字 $x_1,\cdots,x_n$, $\cdots$的多项式环）. 则 $R=R\cdot 1$ 为一元生成的 R-模. 但是理想 $(x_1,x_2,\cdots,x_n,\cdots)$ 作为 R-模不是有限生成的.

例 2 设 p 为固定的素数，$G=\{\bar{x}\in\mathbf{Q}/\mathbf{Z}\mid x\in\mathbf{Q}$，存在 $n\geqslant 1$，使得 $p^n x\in\mathbf{Z}\}$. 即 G 是 $\mathbf{Q}/\mathbf{Z}$ 中阶为素数 p 的方幂的全部元素组成的集合. 这是加法 Abel 群. 对于每个 $n\geqslant 0, G_n=\frac{1}{p^n}\mathbf{Z}/\mathbf{Z}$ 是 G 的 p^n阶子群. 并且 $G_0\subset G_1\subset G_2\subset\cdots\subset G_n\subset\cdots$. 于是 G不为Noether $\mathbf{Z}$-模. $\left(\text{或者由 } G=\bigcup_{n>0} G_n \text{ 本身不是有限生成的，也可知道 } G \text{ 不是 Noether}\mathbf{Z}\text{-模.}\right)$

为了得到 Noether 模更多的例子，我们需要研究这种模的一些基本性质.

引理 7 设 $0\to M'\xrightarrow{\alpha}M\xrightarrow{\beta}M''\to 0$ 是 R-模短正合序列，则：M 为 Noether R-模 $\Longleftrightarrow M'$ 和 M'' 均是 Noether R-模.

证明 $\Rightarrow$：设 $N_1'\subseteq N_2'\subseteq\cdots\subseteq N_n'\subseteq\cdots$ 是 M' 的子模升链，则 $\alpha(N_1')\subseteq\alpha(N_2')\subseteq\cdots\subseteq\alpha(N_n')\subseteq\cdots$ 是 M 的子模升链. 如果 M 为 Noether 模，则后一升链是稳定的. 由于 α 为单同态，从而前一升链也是稳定的. ($\alpha(N_n')=\alpha(N_{n+1}')\Rightarrow N_n'=N_{n+1}'$). 于是 M' 为 Noether 模.

设 $N_1''\subseteq N_2''\subseteq\cdots\subseteq N_n''\subseteq\cdots$ 是 M'' 的子模升链，则 $\beta^{-1}(N_1'')\subseteq\beta^{-1}(N_2'')\subseteq\cdots\subseteq\beta^{-1}(N_n'')\subseteq\cdots$ 是 M 的子模升链. 由于 β 为满同态可知 $\beta(\beta^{-1}(N_n''))=N_n''$. 从而若后一升链是稳定的可推出前一升链也是稳定的. 于是由 M 为 Noether 模可得出 M'' 为 Noether 模的结论.

$\Leftarrow$：为了符号简单，我们不妨设 M' 为 M 的子模，而 α 为包含映射，$M''=M/M'$ 而 β 是标准满同态. 假设 M' 和 M'' 均为 Noether 模. 对于 M 的子模升链 $N_1\subseteq N_2\subseteq\cdots\subseteq N_n\subseteq\cdots$，则 $\alpha^{-1}(N_1)\subseteq\alpha^{-1}(N_2)\subseteq\cdots\subseteq\alpha^{-1}(N_n)\subseteq\cdots$，和 $\beta(N_1)\subseteq\cdots\subseteq\beta(N_n)\subseteq\cdots$ 分别是 M' 和 M'' 中的子模升链. 在我们上述规定下，$\alpha^{-1}(N_i)=N_i\cap M'$，$\beta(N_i)=\bar{N}_i$（$N_i$ 在 $M/M'=M''$ 中的标准同态象）. 由于后两个升链是稳定的，从而有 $n_0\geqslant 1$ 使得

$$N_{n_0}\cap M'=N_{n_0+1}\cap M'=\cdots,\ \bar{N}_{n_0}=\bar{N}_{n_0+1}=\cdots$$

但是由模的同态基本定理，$\bar{N}_m\cong\dfrac{N_m+M'}{M'}\cong\dfrac{N_m}{N_m\cap M'}\ (m\geqslant 1)$.

于是我们有 $N_{n_0}=N_{n_0+1}=\cdots$. 这就表明 M 是 Noether 模. ▌

系 1 若 $M_i\,(1\leqslant i\leqslant n)$ 均为 R-模，则：$\bigoplus\limits_{i=1}^{n}M_i$ 为 Noether R-模 $\Longleftrightarrow M_i\,(1\leqslant i\leqslant n)$ 均为 Noether R-模.

证明 将引理 7 用于正合序列 $0\to M_n\to\bigoplus\limits_{i=1}^{n}M_i\to\bigoplus\limits_{i=1}^{n-1}M_i\to 0$,

然后对 n 归纳即可. ▌

系 2 若 M 是 Noether R-模，则 M 的每个子模和商模也均是 Noether 模.

证明 将引理 7 用于正合序列 $0\to M'\to M\to M/M'\to 0$. ▌

定义 如果环 R 是 Noether R-模，我们便称 R 为 Noether 环.

根据定理 5，可知环 R 是 Noether 环，当且仅当下面三个等价条件的任何一个成立的时候：

(1) R 的每个理想均是有限生成的；

(2) R 中理想升链必是稳定的；

(3) R 的一个理想集合如果非空，则必有极大元.

例 3 每个域均是 Noether 环，因为域 F 只有两个理想：$F=(1)$ 和 (0). 每个主理想环 R 均是 Noether 环，因为 R 中理想均是一元生成的. 特别地，$\mathbf{Z}$，$\mathbf{Z}/n\mathbf{Z}(n\geqslant 1)$，$k[x]$（$k$ 为域）均为 Noether 环. 当然，每个有限环均是 Noether 环.

例 4 例 1 后面的注记表明 $R=k[x_1,x_2,\cdots,x_n,\cdots]$（$k$ 为域）不是 Noether 环. 但是 R 为整环，它的商域 K 是 Noether 环（例 3），而 R 为 K 的子环. 这例子表明，一个 Noether 环的子环不必为 Noether 环（这与 Noether 模的情形不同. 为什么会有此差别?）. 但是另一方面我们有

引理 8 Noether 环的商环必然是 Noether 环.

证明 设 R 为 Noether 环，则它是 Noether R-模. 对于 R 的每个理想 $\mathfrak{a}$，由引理 7 的系 2 可知 $R/\mathfrak{a}$ 为 Noether R-模. 但是由于 $R/\mathfrak{a}$ 看作为 R-模和看作为 $R/\mathfrak{a}$-模，其结构是一样的. 比如说，$R/\mathfrak{a}$ 的一个 R-子模和一个 $R/\mathfrak{a}$-子模是一回事. 因此 $R/\mathfrak{a}$ 也为 Noether $R/\mathfrak{a}$-模. 即 $R/\mathfrak{a}$ 是 Noether 环. ▌

引理 9 设R为Noether环，M为有限生成R-模，则M为Noether R-模.

证明 由假设知M为R^n（对某个$n\geq1$）的商模. 由于R是Noether环，从而R为Noether R-模. 由此知R^n也是Noether R-模(引理7的系1). 于是其商模M也是Noether R-模(引理7的系2). ▌

注记 例1后面的注记表明，如果R不是Noether环，则引理9不再成立.

系 设A为环B的子环，并且A是Noether环. 如果B是有限生成A-模，则B也是Noether环.

证明 由引理9知道B为Noether A-模，从而更是Noether B-模. 即B为Noether环. ▌

例 5 环$\mathbf{Z}[\sqrt{-10}]=\{a+b\sqrt{-10}\mid a,\ b\in\mathbf{Z}\}=\mathbf{Z}\oplus\mathbf{Z}\sqrt{-10}$为有限生成$\mathbf{Z}$-模，从而由上面的系可知这是Noether环.

下一个引理表明算子S^{-1}保持环的Noether特性.

引理 10 设S是环R的乘法集. 如果R是Noether环，则$S^{-1}R$也是Noether环.

证明 我们从第三章知道，$S^{-1}R$中每个理想均有形式$S^{-1}\mathfrak{a}$，其中$\mathfrak{a}$为R的理想. 如果R是Noether环，则$\mathfrak{a}$是有限生成理想，即$\mathfrak{a}=Rx_1+\cdots+Rx_n$. 于是$S^{-1}\mathfrak{a}=S^{-1}Rx_1+\cdots+S^{-1}Rx_n$. 从而$S^{-1}R$中每个理想均是有限生成的. 这表明$S^{-1}R$是Noether环. ▌

下面定理对于代数几何是很基本的.

定理 6(Hilbert 基定理) 如果R是Noether环，则多项式环$R[x_1,x_2,\cdots,x_n]$($n\geq1$)也是Noether环.

证明 设$\mathfrak{a}$是$R[x]$的理想. 考虑集合

$$I=\{a\in R \mid \text{存在 } f(x)\in\mathfrak{a} \text{ 使得 } f(x) \text{的首项系数是 } a\}.$$

易知 I 为 R 的理想，从而是有限生成的，$I=Ra_1+\cdots+Ra_n$. 于是对每个 a_i，均有 $f_i(x)\in\mathfrak{a}$ 使得 $f_i(x)=a_ix^{r_i}+cx^{r_i-1}+\cdots(1\leqslant i\leqslant n)$. 记 $r=\max\{r_1,\cdots,r_n\}$. 令 $\mathfrak{a}'$ 为 $f_1,\cdots,f_n$ 在 $R[x]$ 中生成的理想，则 $\mathfrak{a}'\subseteq\mathfrak{a}$. 现在对每个多项式 $f(x)=ax^m+\cdots\in\mathfrak{a}$，

有 $a\in I$. 于是 $a=\sum_{i=1}^{n}u_ia_i, u_i\in R$. 如果 $m\geqslant r$，则

$$f'(x)=f(x)-\sum_{i=1}^{n}u_if_i(x)x^{m-r_i}\in\mathfrak{a},$$

$$\sum_{i=1}^{n}u_if_i(x)x^{m-r_i}\in\mathfrak{a}',$$

并且 $\deg f'(x)<m$，如果 $\deg f'(x)$ 仍然大于 r，则再如此继续作下去. 从而我们总可以求得多项式 $h(x)\in\mathfrak{a}'$，使得 $f(x)=g(x)+h(x)$，而 $\deg g(x)<r$. 令 $M=R\oplus Rx\oplus\cdots\oplus Rx^{r-1}$，则 $g(x)\in\mathfrak{a}\cap M$. 于是我们证明了

$$\mathfrak{a}=(\mathfrak{a}\cap M)+\mathfrak{a}'. \tag{1}$$

但是 M 为有限生成 R-模，而 R 为 Noether 环，从而 M 为 Noether R-模(引理 9). 于是它的子模 $\mathfrak{a}\cap M$ 是有限生成 R-模. 令 $\mathfrak{a}\cap M=Rg_1+\cdots+Rg_m$. 则由(1)式可知

$$\mathfrak{a}=Rg_1+\cdots+Rg_m+R[x]f_1+\cdots+R[x]f_n\subseteq R[x]g_1+\cdots+R[x]g_m+R[x]f_1+\cdots+R[x]f_n\subseteq\mathfrak{a}.$$

从而 $\mathfrak{a}$ 是 $R[x]$ 中由 $\{g_1,\cdots,g_m,f_1,\cdots,f_n\}$ 生成的理想. 因此 $R[x]$ 为 Noether 环.

再用数学归纳法可知 $R[x_1,\cdots,x_n]$ 为 Noether环. ▍

例 6 由定理 6 可知，若 k 为域，则 $k[x_1,\cdots,x_n]$ 为 Noether 环. 在代数几何中我们主要使用这个 Noether 环. 此外，$\mathbf{Z}[x_1,\cdots,x_n]$，$\mathbf{Z}/n\mathbf{Z}[x_1,\cdots,x_n]$ 等也均是 Noether 环.

以上我们给出构作Noether环的许多方法．现在我们的目标是要证明 Noether 环中每个理想均是可分解的，即均有极小准素分解式．

定义 环R中理想$\mathfrak{a}$叫作是**不可约的**，是指：如果 $\mathfrak{a}=\mathfrak{b}\cap\mathfrak{c}$（两个理想之交），则$\mathfrak{a}=\mathfrak{b}$或者$\mathfrak{a}=\mathfrak{c}$．

否则，如果存在$\mathfrak{b}$和$\mathfrak{c}$使得$\mathfrak{a}=\mathfrak{b}\cap\mathfrak{c}$（两个理想之交），并且$\mathfrak{a}\subset\mathfrak{b}$，$\mathfrak{a}\subset\mathfrak{c}$，则称$\mathfrak{a}$是**可约的**．

引理 11 Noether 环R中每个理想均是有限个不可约理想之交．

证明 如果R中存在着理想不能表成有限个不可约理想之交，则这样的理想组成的集合Σ就是非空的．从而有极大元$\mathfrak{a}$，显然$\mathfrak{a}$必然可约．从而$\mathfrak{a}=\mathfrak{b}\cap\mathfrak{c}$，$\mathfrak{a}\subset\mathfrak{b}$，$\mathfrak{a}\subset\mathfrak{c}$．由于$\mathfrak{a}$的极大性可知$\mathfrak{b}$，$\mathfrak{c}\notin\Sigma$，从而均可表成有限个不可约理想之交：$\mathfrak{b}=\mathfrak{p}_1\cap\cdots\cap\mathfrak{p}_n$，$\mathfrak{c}=\mathfrak{q}_1\cap\cdots\cap\mathfrak{q}_m$（$\mathfrak{p}_i$，$\mathfrak{q}_j$均不可约）．于是 $\mathfrak{a}=\mathfrak{b}\cap\mathfrak{c}=\mathfrak{p}_1\cap\cdots\cap\mathfrak{p}_n\cap\mathfrak{q}_1\cap\cdots\cap\mathfrak{q}_m$ 也是有限个不可约理想之交，这就与$\mathfrak{a}\in\Sigma$矛盾．从而引理 11 必然成立．▌

引理 12 Noether环R中的不可约理想必为准素理想．

证明 设$\mathfrak{a}$是R中的不可约理想．由于R中包含$\mathfrak{a}$的理想$\mathfrak{b}$和$R/\mathfrak{a}$中的理想$\overline{\mathfrak{b}}=\mathfrak{b}/\mathfrak{a}$之间保序一一对应，可知(0)为$R/\mathfrak{a}$中的不可约理想．并且由于$\mathfrak{b}$为$R$中准素理想($\mathfrak{b}\supseteq\mathfrak{a}$)$\Longleftrightarrow\overline{\mathfrak{b}}$为$R/\mathfrak{a}$中准素理想．从而只需对$\mathfrak{a}=(0)$的情形证明引理 12 即可．即：若(0)为$R$中不可约理想，我们来证明(0)准素．设$x,y\in R$，$xy=0$，$y\neq0$．考虑$R$中理想升链：

$$\mathrm{Ann}(x)\subseteq\mathrm{Ann}(x^2)\subseteq\cdots\subseteq\mathrm{Ann}(x^n)\subseteq\cdots$$

由于R是 Noether 环，从而有$n\geqslant1$使得$\mathrm{Ann}(x^n)=\mathrm{Ann}(x^{n+1})=\cdots$．我们有$(x^n)\cap(y)=(0)$，这是由于：如果$a\in(x^n)\cap(y)$，则$ax\in(xy)=(0)$，于是$ax=0$，又$a=bx^n(b\in R)$．从而$bx^{n+1}=ax=0$．于是$b\in\mathrm{Ann}(x^{n+1})=\mathrm{Ann}(x^n)$．从而 $a=bx^n=0$．这

就表明$(x^n)\cap(y)=(0)$. 但已假定(0)不可约，而$(y)\neq(0)$. 从而必然$(x^n)=(0)$. 即$x^n=0$. 这又表明(0)是准素的. ▌

由引理 11 和引理 12 立刻得出：

定理 7 Noether 环中每个理想均是可分解的. 即均有（极小）准素分解式. ▌

本节最后我们再证明 Noether 环的一些特殊性质.

引理 13 在 Noether 环R中，每个理想$\mathfrak{a}$均包含$\sqrt{\mathfrak{a}}$的某个幂.

证明 设$x_1,\cdots,x_k$生成理想$\sqrt{\mathfrak{a}}$，则有$n_i\geqslant 1$，使得$x_i^{n_i}\in\mathfrak{a}$ $(1\leqslant i\leqslant k)$. 令$m=n_1+\cdots+n_k$. 则$(\sqrt{\mathfrak{a}})^m$是由元素$\{x_1^{r_1}\cdots x_k^{r_k}\mid r_1+\cdots+r_k=m\}$生成的. 当$r_1+\cdots+r_k=m$时至少有一个$r_i\geqslant n_i$. 从而$x_1^{r_1}\cdots x_k^{r_k}\in\mathfrak{a}$. 这就表明$(\sqrt{\mathfrak{a}})^m\subseteq\mathfrak{a}$. ▌

注记 若R不是 Noether 环，则引理 13 不再成立. 例$R=k[x_1,x_2,\cdots,x_n,\cdots]$, $\mathfrak{a}=(x_1, x_2^2,\cdots, x_n^n,\cdots)$. 则$\sqrt{\mathfrak{a}}=(x_1, x_2,\cdots,x_n,\cdots)$. 从而$\mathfrak{a}$不包含$\sqrt{\mathfrak{a}}$的任何幂.

在引理 13 中取$\mathfrak{a}=(0)$，即知

系 Noether 环的小根$\sqrt{(0)}$（全部幂零元组成的理想）是幂零理想（即有m，使$(\sqrt{(0)})^m=(0)$）. ▌

引理 14 设$\mathfrak{m}$是 Noether 环R中的极大理想，$\mathfrak{q}$为R的理想. 则下面三条件彼此等价.

(1) $\mathfrak{q}$为$\mathfrak{m}$-准素理想；

(2) $\sqrt{\mathfrak{q}}=\mathfrak{m}$；

(3) 存在$n\geqslant 1$使得$\mathfrak{m}^n\subseteq\mathfrak{q}\subseteq\mathfrak{m}$.

证明 (1)⇒(2)显然. (2)⇒(1)由引理 2. (2)⇒(3)由引理 13. (3)⇒(2)由$\mathfrak{m}^n\subseteq\mathfrak{q}\subseteq\mathfrak{m}$取根得到$\mathfrak{m}\subseteq\sqrt{\mathfrak{q}}\subseteq\mathfrak{m}$，即$\sqrt{\mathfrak{q}}=\mathfrak{m}$.
▌

引理 15 设 $\mathfrak{a}$ 是 Noether环 R 中的真理想. 则:属于 $\mathfrak{a}$ 的素理想全体 $=\{\mathfrak{p}\in \mathrm{Spec}\,R \mid$ 有 $x\in R$ 使得 $\mathfrak{p}=(\mathfrak{a}:x)\}$.

证明 象引理 12 的证明那样,通过转入商环 $R/\mathfrak{a}$, 我们可以一开始就设 $\mathfrak{a}=(0)$. 令 $(0)=\bigcap_{i=1}^{n}\mathfrak{q}_i$ 为极小准素分解式, $\mathfrak{p}_i=\sqrt{\mathfrak{q}_i}$. 我们要证明: $\{\mathfrak{p}_1,\cdots,\mathfrak{p}_n\}=\{\mathfrak{p}\in \mathrm{Spec}\,R \mid$ 存在 $x\in R$ 使得 $\mathfrak{p}=\mathrm{Ann}(x)\}$. 令 $\mathfrak{a}_i=\bigcap_{\substack{j=1\\ j\neq i}}^{n}\mathfrak{q}_j\neq(0)$. 由定理 1 的证明可知对 $0\neq x\in\mathfrak{a}_i$, 则有 $\sqrt{\mathrm{Ann}(x)}=\mathfrak{p}_i$. 从而 $\mathrm{Ann}(x)\subseteq\mathfrak{p}_i$. 但是由引理 13 可知有 $m\geqslant 1$ 使得 $\mathfrak{p}_i^m\subseteq\mathfrak{q}_i$. 于是 $\mathfrak{a}_i\mathfrak{p}_i^m\subseteq\mathfrak{a}_i\cap\mathfrak{p}_i^m\subseteq\mathfrak{a}_i\cap\mathfrak{q}_i=(0)$. 即 $\mathfrak{a}_i\mathfrak{p}_i^m=(0)$. 设 m 是使 $\mathfrak{a}_i\mathfrak{p}_i^m=(0)$ 的最小正整数 (由 $\mathfrak{a}_i\neq(0)$ 可知 $m\geqslant 1$). 从而 $\mathfrak{a}_i\mathfrak{p}_i^{m-1}\neq(0)$. 于是存在 $0\neq y\in\mathfrak{a}_i\mathfrak{p}_i^{m-1}$. 从而 $y\mathfrak{p}_i=(0)$, 即 $\mathrm{Ann}(y)\supseteq\mathfrak{p}_i$. 但是 $0\neq y\in\mathfrak{a}_i$. 从而将 y 看成前面的 x, 则又有 $\mathrm{Ann}(y)\subseteq\mathfrak{p}_i$. 从而对于如此选取的 y, 我们有 $\mathrm{Ann}(y)=\mathfrak{p}_i$.

反之,如果 $\mathrm{Ann}(x)=\mathfrak{p}\in\mathrm{Spec}\,R$, $x\neq 0$. 则 $\sqrt{\mathrm{Ann}(x)}=\mathfrak{p}$. 由定理 1 可知 $\mathfrak{p}$ 为属于 (0) 的素理想. ▌

习　题

1. 设 R 不是 Noether 环, Σ 为 R 中不是有限生成的理想的全体. 求证 Σ 有极大元,并且每个极大元均是素理想. [提示: 设 $\mathfrak{a}$ 为 Σ 中极大元. $x,y\in R$, $xy\in\mathfrak{a}$, 如果 $x\notin\mathfrak{a}$, $y\notin\mathfrak{a}$. 证明存在有限生成理想 $\mathfrak{a}_0\subseteq\mathfrak{a}$, 使得 $\mathfrak{a}_0+xR=\mathfrak{a}+xR$, $\mathfrak{a}=\mathfrak{a}_0+x\cdot(\mathfrak{a}:x)$ 但是 $(\mathfrak{a}:x)$ 为有限生成理想. 从而 $\mathfrak{a}$ 也为有限生成理想,这就导致矛盾.]

2. (I. S. Cohen) 环 R 为 Noether 环 $\Longleftrightarrow R$ 的每个素理想均有限生成.

3. 设 $\mathfrak{a}$ 为环 R 的不可约理想,则下列三命题彼此等价:

(1) $\mathfrak{a}$ 为准素理想.

(2) 对于R的每个乘法集 S,均有 $x\in S$ 使得$(S^{-1}\mathfrak{a})^c=(\mathfrak{a}:x)$.

(3) 对于每个$x\in R$,R 的理想升链$(\mathfrak{a}:x)\subseteq(\mathfrak{a}:x^2)\subseteq\cdots\subseteq(\mathfrak{a}:x^n)\subseteq\cdots$ 是稳定的.

4. 若 $R[x]$为 Noether 环,试问R是否必为 Noether 环.

5. 如果环R满足以下两条件,求证R为 Noether 环.

(a) 对每个 $\mathfrak{m}\in \mathrm{Max}\,R$,$R_{\mathfrak{m}}$为 Noether 环;

(b) 对每个 $0\neq x\in R$,$\{\mathfrak{m}\in\mathrm{Max}\,R\mid x\in\mathfrak{m}\}$为有限集.

[提示:设 $\mathfrak{a}$ 为R的理想,$\mathfrak{a}\neq(0)$. 令$\{\mathfrak{m}_1,\cdots,\mathfrak{m}_r\}=\{\mathfrak{m}\in\mathrm{Max}\,R\mid\mathfrak{m}\supseteq\mathfrak{a}\}$.取 $0\neq x_0\in\mathfrak{a}$.令$\{\mathfrak{m}_1,\cdots,\mathfrak{m}_r,\mathfrak{m}_{r+1},\cdots,\mathfrak{m}_{r+s}\}=\{\mathfrak{m}\in\mathrm{Max}\,R\mid x_0\in\mathfrak{m}\}$.则有 $x_j\in\mathfrak{a}$使$x_j\notin\mathfrak{m}_{r+j}(1\leqslant j\leqslant s)$.由于 $R_{\mathfrak{m}_i}(1\leqslant i\leqslant r)$为 Noether 环,从而有$x_{s+1},\cdots,x_t\in\mathfrak{a}$,使它们在 $R_{\mathfrak{m}_i}$ 中的象生成 $S_i^{-1}\mathfrak{a}$ $(S_i=R-\mathfrak{m}_i,1\leqslant i\leqslant r)$.令 $\mathfrak{a}_0=(x_0,\cdots,x_t)$.证明对于每个$\mathfrak{m}\in\mathrm{Max}\,R$, $\mathfrak{a}_0$ 和 $\mathfrak{a}$ 在 $R_{\mathfrak{m}}$中扩张成同一理想. 于是 $\mathfrak{a}=\mathfrak{a}_0=(x_0,\cdots,x_t)$.]

6. 设B为有限生成 R-模. 则:B 为 Noether R-模$\Longleftrightarrow R/\mathrm{Ann}\,(B)$ 为 Noether 环.

7. 设环R中每个极大理想均可写成 cR,其中 $c\in R,c^2=c$. 求证:

(1) R中准素理想必为极大理想.

(2) R 为 Noether 环. [提示:利用习题 2.]

8. 设R为 Noether 环. $\mathfrak{p}\in\mathrm{Spec}\,R-\mathrm{Max}\,R$.$\mathfrak{q}\neq\mathfrak{p}$, 并且 $\mathfrak{q}$ 为 $\mathfrak{p}$-准素理想. 求证有理想 $\mathfrak{a}$,$\mathfrak{p}\supset\mathfrak{a}\supset\mathfrak{q}$,并且 $\mathfrak{a}$ 不是准素理想.

9. 设R为 Noether 整环,$(0)\neq\mathfrak{p}\in\mathrm{Spec}\,R$. 求证 $\mathfrak{p}^2\neq\mathfrak{p}$.

10. 设 $\mathfrak{a}_1,\cdots,\mathfrak{a}_n$ 为环R的理想,且$\bigcap\limits_{i=1}^{n}\mathfrak{a}_i=(0)$. 如果 $R/\mathfrak{a}_i$ $(1\leqslant i\leqslant n)$ 均是 Noether 环,求证R也是 Noether 环.

11. 设 a 为域F中任意元素. 求证 $(x^2,\ xy)=(x)\cap(y-ax,\ x^2)$ 是 Noether 环 $F[x,y]$中理想(x^2,xy)的极小准素分解式.

§ 4.3 Artin 模和 Artin 环

根据定理 5，Noether 模可以用极大条件或升链条件来定义，完全对偶地我们有

引理 16 设M为R-模，则下面两条件等价：

(1)（降链条件） M 的每个 R-子模降链 $N_1 \supseteq N_2 \supseteq \cdots \supseteq N_n \supseteq \cdots$ 都是稳定的，即存在 n_0，使得 $N_{n_0} = N_{n_0+1} = \cdots$.

(2)（极小条件） M 的一个子模集合如果非空，则必有极小元.

证明 (1)⇒(2)：象定理 5 那样用反证法.

(2)⇒(1)：对于(1)中所给的子模降链，令 $\Sigma = \{N_n \mid n \geqslant 1\}$，则 Σ 应当有极小元．设极小元为 N_{n_0}，则 $N_{n_0} = N_{n_0+1} = \cdots$. ▌

定义 满足引理 16 中降链条件或极小条件的 R-模叫作是 Artin R-模.

注记 我们最初定义 Noether 模是用有限性条件(即每个子模都是有限生成的)，Artin 模没有与之类似的定义方式．但是，凡是用升链条件或者极大条件得出的 Noether 环的性质，均应当期望 Artin 模也有相应的性质．下面就是其中的一些.

引理 17 如果 $0 \to M' \to M \to M'' \to 0$ 是 R-模短正合序列，则：M 为 Artin R-模 $\Longleftrightarrow M'$ 和 M'' 均为 Artin R-模.

证明 仿照引理 7 的证明，但是将升链改为降链. ▌

系 1 设 $M_i (1 \leqslant i \leqslant n)$ 均为 R-模，则：$\bigoplus_{i=1}^{n} M_i$ 为 Artin R-模 $\Longleftrightarrow M_i (1 \leqslant i \leqslant n)$ 均为 Artin R-模. ▌

系 2 Artin R-模的每个子模和商模也是 Artin R-模. ▌

例 1 每个有限 Abel 群既是 Noether Z-模也是 Artin Z-模．每个域 R 既是 Noether R-模也是 Artin R-模.

例 2 Z 为 Noether Z-模但不为 Artin Z-模（考虑降链

$(2)\supset(2^2)\supset\cdots\supset(2^n)\supset\cdots)$.

例 3 §4.2 中例 2 的 Abel 群 $G=\bigcup_{n=0}^{\infty}G_n, G_n=\frac{1}{p^n}\mathbf{Z}/\mathbf{Z}$ 不是 Noether Z-模. 但它是 Artin Z-模. 因为不难证明, G 的真子群必为有限群. 从而 G 不可能有不稳定的子群降链.

例 4 $R=k[x_1,\cdots,x_n,\cdots]$($k$ 为域) 既不是 Noether R-模, 也不是 Artin R-模(考虑降链 $(x_1)\supset(x_1^2)\supset\cdots(x_1^n)\supset\cdots$).

一个 R-模 M 如果同时是 Noether R-模和 Artin R-模, 则有一个重要的性质: M 有组成列.

定义 设 M 为 R-模, $M\neq(0)$. 如果 M 除了 (0) 和 M 本身之外没有别的子模, 我们称 M 为**单 R-模**.

例如: 每个素数阶循环群均是单 Z-模; 主理想整环 R 如果不是域, 则 R 上的模 M 为单模 $\Longleftrightarrow M$ 同构于循环 R-模 $R/(a)$, 其中 a 为 R 的素元; 域 K 上的向量空间 V 为单 K-模 $\Longleftrightarrow \dim_K V=1$.

定义 设 M 为 R-模. $M=M_0\supset M_1\supset\cdots\supset M_n=(0)$ 为 M 的有限个子模形成的严格递降子模链 (以 M 开头以 (0) 结尾). 如果 $M_{i-1}/M_i(1\leqslant i\leqslant n)$ 均是单 R-模, 我们称此链为 R-模的**合成列**. 而 n 叫作是该合成列的**长度**.

引理 18 如果 R-模 M 有合成列, 则 M 的所有合成列均有相同的长度, 并且 M 的每个严格递降子模链均可嵌到某个合成列之中(即可在链的某些位置上适当加进一些子模, 使之变成一个合成列).

证明 以 $l(M)$ 表示模 M 所有合成列的最小长度 (由于 M 具有合成列, 从而 $l(M)$ 为非负整数). 我们先证明两件事情:

(A) 若N为M的 R-子模,并且是 M 的真子模(即 $N\subset M$),则N也有合成列,并且 $l(N)<l(M)$. 这是因为:假如 $M=M_0\supset M_1\supset\cdots\supset M_{l(M)}=(0)$为 M 的合成列. 令 $N_i=N\cap M_i$. 我们有自然的 R-模单同态 $N_{i-1}/N_i\to M_{i-1}/M_i$(作自然同态 $N_{i-1}\to M_{i-1}/M_i$,其核为 $N_{i-1}\cap M_i=N\cap M_{i-1}\cap M_i=N\cap M_i=N_i$). 于是 N_{i-1}/N_i 或者为(0)(即 $N_{i-1}=N_i$),或者同构于单模 M_{i-1}/M_i. 从而在 $N=N_0\supseteq N_1\supseteq\cdots\supseteq N_{l(M)}=(0)$中去掉重复项之后,便给出 R-模N的一个合成列. 同时证明了 $l(N)\leqslant l(M)$. 如果 $l(N)=l(M)$,则必然 $\dfrac{N_{i-1}}{N_i}\cong\dfrac{M_{i-1}}{M_i}(1\leqslant i\leqslant l(M))$. 由此和"初始条件"$M_{l(M)}=N_{l(M)}=(0)$以及 $M_i\supseteq N_i$ 可以递归地得到 $M_{n-1}=N_{n-1},\cdots,M=M_0=N_0=N$. 这与假设矛盾. 于是 $l(N)<l(M)$,

(B) M 的每个严格递降子模链 $M=M_0\supset\cdots\supset M_k=(0)$ 的长度 k 均不超过 $l(M)$. 这是由于从(A)推得 $l(M)>l(M_1)>\cdots>l(M_k)=0$. 于是 $k\leqslant l(M)$.

现在证明引理 18:设M的某个合成列长度为 k. 由(B)可知 $k\leqslant l(M)$. 而由 $l(M)$的极小性即知 $k=l(M)$. 从而 M 的每个合成列都有同样的长度. 另一方面,对于 M 的每个子模链 $M=M_0\supset M_1\supset\cdots\supset M_k=(0)$. 如果 $k<l(M)$,则它不为合成列. 于是必有某个 M_{i-1}/M_i 不为单模,从而有子模 M'/M_i 使得 $M_{i-1}\supset M'\supset M_i$. 将 M' 放到原来子模链中,长度增加1. 如此继续下去,一直到长度为 $l(M)$,则它必为合成列. 这就证明了引理 18. ▌

引理 19 R-模M有合成列$\Longleftrightarrow M$同时为 Noether R-模和 Artin R-模.

证明 $\Rightarrow$:由引理 18 可知若 R-模有合成列,则 M 不可能有无限严格升或严格降的子模链. 从而必同时为 Noether 模和

Artin 模.

$\Leftarrow$:不妨设 $M\neq(0)$. 令 $\Sigma=\{M$ 的子模 $N\mid N\neq M\}$. 由于 M 是 Noether 模则 Σ 有极大元 M_1. 于是 M_1 为 $M=M_0$ 的极大真子模,从而 M_0/M_1 必为单模. 同样地,若 $M_1\neq(0)$,则 M_1 又有极大真子模 M_2,于是 M_1/M_2 为单模. 由此可得到 $M=M_0\supset M_1\supset\cdots\supset M_n\supset\cdots$,使得 M_{i-1}/M_i 均为单模. 又由于 M 是 Artin 模,从而必然有某个 M_n 为(0). 于是 $M=M_0\supset M_1\supset\cdots\supset M_n=(0)$即是$M$的一个合成列. ▌

定义 设R-模M有合成列. 由引理 18 知M的所有合成列有公共的长度 $l(M)$. 我们将 $l(M)$叫作是**模 M 的长度**. 若 M 没有合成列,也称 M 的长度无限,记成 $l(M)=+\infty$.

引理 20 设 $0\to M'\xrightarrow{\alpha}M\xrightarrow{\beta}M''\to 0$ 为 R-模正合序列. 则 M 的长度有限$\Longleftrightarrow M'$ 和 M'' 的长度均有限. 并且在这种情形下,$l(M)=l(M')+l(M'')$.

证明 设

$$M'=M_0'\supset M_1'\supset\cdots\supset M_k'=(0), \tag{1}$$

$$M''=M_0''\supset M_1''\supset\cdots\supset M_l''=(0) \tag{2}$$

分别是 M' 和 M'' 的子模链,则我们有 M 的长为 $l+k$ 的子模链

$$M=\beta^{-1}(M'')\supset\beta^{-1}(M_1'')\supset\cdots\supset\beta^{-1}(M_{l-1}'')\supset\underset{\alpha(M')}{\underset{\|}{\beta^{-1}(0)}}\supset$$

$$\supset\alpha(M_1')\supset\cdots\supset\alpha(M_k')=(0). \tag{3}$$

并且

$$\alpha(M_{i-1}')/\alpha(M_i')\cong M_{i-1}'/M_i', \tag{4}$$

$$\beta^{-1}(M_{j-1}'')/\beta^{-1}(M_j'')\cong M_{j-1}''/M_j''.$$

如果 M' 和 M'' 有一个是长度无限的,则 l 和 k 至少有一个可任意大,从而 $k+l$ 可任意大. 于是M也是长度无限的. 反之,若 M' 和 M'' 长度均有限. 设(1)和(2)分别是 M' 和 M'' 的合成列,则

由于(4)式可知(3)为 M 的合成列. 因此 $l(M)=l+k=l(M')+l(M'')$. ▌

系 设 $0\to M_1\xrightarrow{\alpha_1}M_2\xrightarrow{\alpha_2}\cdots\xrightarrow{\alpha_{n-1}}M_n\to 0$ 为 R-模正合序列，并且 $M_i(1\leqslant i\leqslant n)$的长度均有限. 则 $\sum_{i=1}^{n}(-1)^i l(M_i)=0$.

证明 系中的正合序列等价于下面两个正合序列：

$$0\to M_1\to\alpha_1(M_1)\to 0 \text{ 和 } 0\to\frac{M_2}{\alpha_1(M_1)}\to M_3\to\cdots\to M_n\to 0.$$

于是由引理 20 并对 n 归纳即可证得此系. ▌

现在我们谈 Artin 环. 其定义与 Noether 环相仿.

定义 环 R 如果是 Artin R-模，则称 R 为 Artin 环.

于是，R 为 Artin 环相当于 R 满足如下两个等价条件之一：

(1) 降链条件：R 的每个理想降链都是稳定的；

(2) 极小条件：R 的一个理想集合如果非空，则必有极小元.

例 1 有限环和域都既是 Noether 环也是 Artin 环.

例 2 $R=k[x_1,\cdots,x_n,\cdots]$($k$ 为域)既不是 Noether 环也不是 Artin 环.

例 3 $\mathbf{Z}$ 为 Noether 环，但不是 Artin 环.

我们没有给出第四种可能性的例子. 事实上，不久我们将要证明(定理 8)：每个 Artin 环都必然是 Noether 环！

整环 $R=k[x_1,\cdots,x_n,\cdots]$不是 Artin 环，但它的商域显然为 Artin 环. 因此，一个 Artin 环的子环不一定为 Artin 环. 但是与 Noether 环一样，我们有

引理 21 Artin 环的商环必为 Artin 环.

证明 仿照引理 8 的证明. ▌

引理 22 设 R 为 Artin 环，M 为有限生成 R-模，则 M 为

Artin R-模.

证明 仿照引理 9 的证明. ▌

系 设 A 为环 B 的子环, 并且 A 为 Artin 环. 如果 B 是有限生成 A-模, 则 B 为 Artin 环. ▌

Artin 环的以下两个特性, 与 Noether 环情形很不一样.

引理 23 Artin 环的素理想必是极大理想.

证明 设 $\mathfrak{p}\in \mathrm{Spec}\, R$ 而 R 为 Artin 环, 则 $B=R/\mathfrak{p}$ 为整环并且 B 也为 Artin 环(引理 21). 对于 $0\neq x\in B$, 由降链条件可知有 n 使得 $(x^n)=(x^{n+1})$. 于是 $x^n=x^{n+1}y$(对某个 $y\in B$). 由于 B 为整环而 $x\neq 0$, 从而 $1=xy$. 这表明 B 中非零元素 x 均是 B 中单位. 从而 B 为域. 于是 $\mathfrak{p}$ 为极大理想. ▌

系 (1) Artin 环的小根等于大根.

(2) Artin 整环必为域. ▌

引理 24 Artin 环 R 中只有有限多个极大理想.

证明 不妨设 $R\neq(0)$. 考虑集合

$$\Sigma=\{\mathfrak{m}_1\cap\cdots\cap\mathfrak{m}_r \mid r\geqslant 1, \mathfrak{m}_i\in \mathrm{Max}\, R\}.$$

由于 R 是 Artin 环, 并且 Σ 非空, 从而 Σ 有极小元 $\mathfrak{m}_1\cap\cdots\cap\mathfrak{m}_n$. 于是对每个 $\mathfrak{m}\in \mathrm{Max}\, R$, 必然 $\mathfrak{m}_1\cap\cdots\cap\mathfrak{m}_n\cap\mathfrak{m}=\mathfrak{m}_1\cap\cdots\cap\mathfrak{m}_n$. 从而 $\mathfrak{m}\supseteq\mathfrak{m}_1\cap\cdots\cap\mathfrak{m}_n\supseteq\mathfrak{m}_1\cdots\mathfrak{m}_n$. 因此有 $i(1\leqslant i\leqslant n)$ 使得 $\mathfrak{m}\supseteq\mathfrak{m}_i$. 但是 $\mathfrak{m},\mathfrak{m}_i$ 为极大理想. 于是 $\mathfrak{m}=\mathfrak{m}_i$. 这就表明 $\mathfrak{m}_1,\cdots,\mathfrak{m}_n$ 为 R 的全部极大理想. ▌

系 Artin 环必为半局部环.

证明 所谓半局部环即是只有有限个极大理想的环. 因此这系由引理 24 立即得出. (事实上, 再由引理 23 可知 Artin 环只有有限个素理想). ▌

Artin 环的下一个性质是 Noether 环也具有的(与引理 13 的

系比较).

引理 25 Artin 环R的小根 $\sqrt{(0)}$是幂零理想.

证明 记 $\mathfrak{n}=\sqrt{(0)}$. 由降链条件知有k使得$\mathfrak{n}^k=\mathfrak{n}^{k+1}=\cdots$,记 $\mathfrak{a}=\mathfrak{n}^k(=\mathfrak{n}^{2k})$. 我们来证明 $\mathfrak{n}^k=\mathfrak{a}=(0)$. 如果$\mathfrak{a}\neq(0)$,考虑集合

$$\Sigma=\{R\text{ 的理想 }\mathfrak{b}\,|\,\mathfrak{a}\mathfrak{b}\neq(0)\}.$$

则 $\mathfrak{a}\in\Sigma$(因为 $\mathfrak{a}^2=\mathfrak{n}^{2k}=\mathfrak{a}\neq(0)$),从而 Σ 为非空集合,于是 Σ 有极小元 $\mathfrak{c}$. 则 $\mathfrak{a}\mathfrak{c}\neq(0)$. 从而有 $x\in\mathfrak{c}$ 使得 $x\mathfrak{a}\neq(0)$. 从而$(x)\in\Sigma$.但是$(x)\subseteq\mathfrak{c}$, 由 $\mathfrak{c}$ 的极小性可知 $\mathfrak{c}=(x)$. 又有 $(x\mathfrak{a})\mathfrak{a}=x\mathfrak{a}^2=x\mathfrak{a}\neq(0)$. 从而$(x\mathfrak{a})\in\Sigma$,$x\mathfrak{a}\subseteq(x)=xR$. 由$(x)=\mathfrak{c}$ 的极小性又得到 $x\mathfrak{a}=xR$. 于是有 $y\in\mathfrak{a}$ 使得 $xy=x\cdot1=x$. 从而 $x=xy=xy^2=\cdots=xy^n=\cdots$. 但是 $y\in\mathfrak{a}=\mathfrak{n}^k\subseteq\mathfrak{n}=\sqrt{(0)}$. 从而有 m 使得 $y^m=0$. 于是 $x=xy^m=0$. 这与 $x\mathfrak{a}\neq(0)$相矛盾. 因此 $\mathfrak{n}^k=\mathfrak{a}=(0)$. ▌

引理 26 如果环R中零理想(0)是有限个极大理想之乘积,则:R为 Noether 环$\Longleftrightarrow R$ 为 Artin 环.

证明 $\Leftarrow$:设$(0)=\mathfrak{m}_1\cdots\mathfrak{m}_n(\mathfrak{m}_i\in\mathrm{Max}R)$. 考虑$R$的$R$-子模链(即理想链):

$$R\supset\mathfrak{m}_1\supseteq\mathfrak{m}_1\mathfrak{m}_2\supseteq\cdots\supseteq\mathfrak{m}_1\mathfrak{m}_2\cdots\mathfrak{m}_n=(0).$$

R-商模 $M_i=\mathfrak{m}_1\cdots\mathfrak{m}_{i-1}/\mathfrak{m}_1\cdots\mathfrak{m}_i$ 被 $\mathfrak{m}_i$ 所零化, 从而 M_i 可看作是 $R/\mathfrak{m}_i$-模. 但是 $R/\mathfrak{m}_i$ 为域,从而 M_i 为 $R/\mathfrak{m}_i$ 上向量空间. 而且 M_i 的 R-模结构和 $R/\mathfrak{m}_i$-向量空间结构是一样的. 如果 R 是 Artin 环,则 R 为 Artin R-模. 从而R的商模$R/\mathfrak{m}_1\cdots\mathfrak{m}_i$ 的子模 $\mathfrak{m}_1\cdots\mathfrak{m}_{i-1}/\mathfrak{m}_1\cdots\mathfrak{m}_i=M_i$ 也是Artin R-模.于是M_i也是Artin $R/\mathfrak{m}_i$-模. 但是对于域 F 上的向量空间 V, 易知: V 为 Artin F-模$\Longleftrightarrow\dim_F V<+\infty\Longleftrightarrow F$-模 V 有合成列. 于是 M_i 作为 $R/\mathfrak{m}_i$-模有合成列, 从而 $M_i=\mathfrak{m}_1\cdots\mathfrak{m}_{i-1}/\mathfrak{m}_1\cdots\mathfrak{m}_i$ 作为 R-模也有合成列. 这也相当于说,在 $\mathfrak{m}_1\cdots\mathfrak{m}_{i-1}$ 和 $\mathfrak{m}_1\cdots\mathfrak{m}_i$ 之间可以加进

有限个中间 R-模之后，使得每相邻两个模之商均是单 R-模. 对于每个 i ($1\leqslant i\leqslant n$)均如此作，就连成 R-模 R 的一个合成列. 于是 R 为Noether R-模(引理 19). 即 R 为 Noether 环.

$\Rightarrow$：与上面证明类似. ▌

定义 设 R 是非零环. 我们称 R 中素理想链 $\mathfrak{p}_0\subset\mathfrak{p}_1\subset\cdots\subset\mathfrak{p}_n$ 的长度为 n. 而 R 中素理想链最大可能的长度，叫作是环 R 的(Krull)**维数**，表示成 $\dim R$.

于是：

(1) 域的维数为 0. 更一般地，$\dim R=0\Longleftrightarrow R$ 中素理想必为极大理想. 因此由引理 23 可知 Artin 环的维数是 0.

(2) $\dim \mathbf{Z}=1$. 更一般地，如果 R 为整环，则：$\dim R=1\Longleftrightarrow$ R 不是域，并且 R 中非零素理想均为极大理想.

我们在下一章要集中研究 $\dim R=1$ 的情形. 现在我们证明一个值得注意的结果.

定理 8 环 R 为 Artin 环$\Longleftrightarrow$环 R 为 Noether 环并且 $\dim R=0$.

证明 $\Rightarrow$：若 R 为 Artin 环，由于素理想均是极大理想(引理 23)，从而 $\dim R=0$. 而且 R 只有有限多个极大理想（引理 24），设它们为 $\mathfrak{m}_1,\cdots,\mathfrak{m}_n$，则 R 的大根和小根均为 $\mathfrak{n}=\mathfrak{m}_1\cap\cdots\cap\mathfrak{m}_n$. 由引理 25 知道有 k 使得 $\mathfrak{n}^k=(0)$. 从而

$$\prod_{i=1}^{n}\mathfrak{m}_i^k\subseteq\left(\bigcap_{i=1}^{n}\mathfrak{m}_i\right)^k=\mathfrak{n}^k=(0).$$

于是 $(0)=\prod_{i=1}^{n}\mathfrak{m}_i^k$. 由引理 26 即知 R 是 Noether 环.

$\Leftarrow$：若 R 为 Noether 环. $(0)=\mathfrak{q}_1\cap\cdots\cap\mathfrak{q}_n$ 为准素分解式，$\mathfrak{p}_i=\sqrt{\mathfrak{q}_i}$. 则 R 的小根为 $\mathfrak{n}=\sqrt{(0)}=\bigcap_{i=1}^{n}\mathfrak{p}_i$. 由引理 13 的系知道有

k 使得 $\mathfrak{n}^k=(0)$. 于是 $\prod_{i=1}^n \mathfrak{p}_i^k=\left(\prod_{i=1}^n \mathfrak{p}_i\right)^k\subseteq\left(\bigcap_{i=1}^n \mathfrak{p}_i\right)^k=\mathfrak{n}^k=(0)$.

从而 $(0)=\prod_{i=1}^n \mathfrak{p}_i^k$. 由 $\dim R=0$ 可知 $\mathfrak{p}_i$ 均为极大理想, 即(0)为有

限多个极大理想之积. 由引理 26 即知 R 为 Artin 环. ▌

最后我们讲 Artin 环的结构定理(定理 9): 每个 Artin 环均可唯一地表示成有限个 Artin 局部环之直和. 我们先谈谈 Artin 局部环的特性. 设 $(R,\mathfrak{m})$ 是 Artin 局部环, 则 R 的唯一极大理想 $\mathfrak{m}$ 即是幂零元全体 $(=\sqrt{(0)})$. $\mathfrak{m}=R-U(R)$, 并且存在 k 使得 $\mathfrak{m}^k=(0)$. 例如 $\mathbf{Z}/p^n\mathbf{Z}$(p 为素数, $n\geqslant1$)均是 Artin局部环. 由定理 8 可知: Artin 局部环$\Longleftrightarrow$维数是 0 的 Noether 局部环. 我们还可以叙述得更具体一些.

引理 27 设 R 为 Noether 局部环, $\mathfrak{m}$ 是 R 的唯一极大理想, 则或者(1) $R\supset\mathfrak{m}\supset\mathfrak{m}^2\supset\cdots\supset\mathfrak{m}^n\supset\cdots$; 或者(2) 有 n 使得 $\mathfrak{m}^n=(0)$. 并且 R 为 Artin 局部环$\Longleftrightarrow$情形(2)成立.

证明 如果 $\mathfrak{m}^n=\mathfrak{m}^{n+1}$. 将 $\mathfrak{m}^n$ 看作是 R-模, 它是有限生成的. 从而由中山引理可知 $\mathfrak{m}^n=(0)$. 这就表明情形(1)和(2)必有且仅有一种情形成立. 对于情形(1), 由于理想链 $R\supset\mathfrak{m}\supset\cdots\supset\mathfrak{m}^n\supset\cdots$ 不稳定, 从而 R 不是 Artin 环. 对于情形(2), 设 $\mathfrak{p}\in\operatorname{Spec}R$, 则 $(0)=\mathfrak{m}^n\subseteq\mathfrak{p}$. 取根即知 $\mathfrak{m}=\mathfrak{p}$. 于是 $\mathfrak{m}$ 也是 R 中唯一素理想, 即 $\dim R=0$. 从而 R 为 Artin 环. ▌

定理 9 (Artin 环结构定理) 每个 Artin 环 R 均可表成有限个 Artin 局部环的直和: $R=R_1\oplus\cdots\oplus R_n$ (R_i 为 Artin 局部环). 如果又有 $R=R_1'\oplus\cdots\oplus R_m'$ (R_i' 均为 Artin 局部环), 则 $n=m$, 并且有 $\{1,2,\cdots,n\}$ 的一个置换 σ, 使得 $R_i\cong R'_{\sigma(i)}$ $(1\leqslant i\leqslant$

n)(环同构).

证明 存在性：根据引理 24，R只有有限多个极大理想：Max $R=\{\mathfrak{m}_1,\cdots,\mathfrak{m}_n\}$. 由定理8的证明可知有$k\geqslant 1$使得$(0)=\prod\limits_{i=1}^{n}\mathfrak{m}_i^k$. 但是 $\mathfrak{m}_i^k(1\leqslant i\leqslant n)$ 两两互素(§1.3，习题 1)，从而$(0)=\bigcap\limits_{i=1}^{n}\mathfrak{m}_i^k$ (§1.2，习题 12). 于是有环的同构 $R\cong R\Big/\bigcap\limits_{i=1}^{n}\mathfrak{m}_i^k\cong\bigoplus\limits_{i=1}^{n}R/\mathfrak{m}_i^k$，而 $R/\mathfrak{m}_i^k$ 为 Artin 局部环.

唯一性：假设$R\cong\bigoplus\limits_{i=1}^{n}R_i$，$R_i$ 均是 Artin 局部环. 令 $\varphi_i: R\to R_i$ 为自然投射，$\mathfrak{a}_i=\mathrm{Ker}\,\varphi_i$. 则 $\mathfrak{a}_i(1\leqslant i\leqslant n)$两两互素，并且$\bigcap\limits_{i=1}^{n}\mathfrak{a}_i=(0)$. 设 $\mathfrak{q}_i$ 为 R_i 的唯一素理想，则$\mathfrak{p}_i=\varphi_i^{-1}(\mathfrak{q}_i)$是$R$的素理想. 因为$R$是 Artin 环，从而 $\mathfrak{p}_i\in\mathrm{Max}\,R$. 但是 $\mathfrak{q}_i$ 为幂零理想. 从而 $\mathfrak{a}^i$ 包含极大理想 $\mathfrak{p}_i$ 的某个幂. 于是 $\mathfrak{a}_i$ 为 $\mathfrak{p}_i$-准素理想. 所以 $(0)=\bigcap\limits_{i=1}^{n}\mathfrak{a}_i$ 为准素分解式. 因为 $\mathfrak{a}_i$ 两两互素，从而 $\mathfrak{p}_i(1\leqslant i\leqslant n)$ 也两两互素. 于是 $\mathfrak{p}_i$ 均是属于(0)的极小素理想. 从而 $\mathfrak{a}_i(1\leqslant i\leqslant n)$均是(0)的孤立准素分支. 由§4.1 定理 4 知 $\mathfrak{a}_i(1\leqslant i\leqslant n)$是由 R所决定的. 从而环 $R_i=R/\mathfrak{a}_i(1\leqslant i\leqslant n)$也由$R$ 所决定. ▎

下一个引理在第五章中是有用的.

引理 28 设$(R,\mathfrak{m})$为 Artin 局部环，$k=R/\mathfrak{m}$. 则以下三条件彼此等价：

(1) R为主理想环；

(2) $\mathfrak{m}$ 为主理想；

(3) $\dim_k(\mathfrak{m}/\mathfrak{m}^2)\leqslant 1$.

证明 (1)⇒(2)显然. (2)⇒(3)：设 $\mathfrak{m}=(a)$. 我们有 R-模满同态

$$f:R\to\frac{\mathfrak{m}}{\mathfrak{m}^2}=\frac{(a)}{(a^2)},x\mapsto\overline{ax}.$$

其核 $\mathrm{Ker}\, f\supseteq\mathfrak{m}=(a)$. 从而诱导出 k-向量空间的线性变换 $\bar{f}:R/\mathfrak{m}\to\mathfrak{m}/\mathfrak{m}^2$，并且 $\bar{f}$ 是满射. 于是 $\dim_k(\mathfrak{m}/\mathfrak{m}^2)\leqslant\dim_k(R/\mathfrak{m})=1$.

(3)⇒(1)：如果 $\dim_k(\mathfrak{m}/\mathfrak{m}^2)=0$，则 $\mathfrak{m}=\mathfrak{m}^2$. 由于 $\mathfrak{m}$ 为有限生成 R-模(Artin 环 R 是Noether 环)，从而由中山引理知 $\mathfrak{m}=(0)$，即 R 为域，当然也是主理想环. 如果 $\dim_k(\mathfrak{m}/\mathfrak{m}^2)=1$，则有 $x\in\mathfrak{m}$，使得 $\mathfrak{m}/\mathfrak{m}^2=k\cdot\bar{x}$. 根据第二章引理 5，可知 $\mathfrak{m}=Rx$，即 $\mathfrak{m}$ 为主理想. 对于 R 的每个真理想 $\mathfrak{a}\neq(0)$. 由于 x 是幂零元素，从而有 $m\geqslant1$ 使得 $x^m=0$. 于是 $\mathfrak{m}^m=(0)$. 于是 $\mathfrak{a}\neq\mathfrak{m}^m=(0)$. 由于 $\mathfrak{a}$ 为真理想，从而 $\mathfrak{a}\subseteq\mathfrak{m}$. 于是存在 $r\geqslant1$ 使得 $\mathfrak{a}\subseteq\mathfrak{m}^r$，$\mathfrak{a}\nsubseteq\mathfrak{m}^{r+1}$. 因此有 $y\in\mathfrak{a}$，$a\in R$ 使得 $y=ax^r$. 但是 $y\notin(x^{r+1})$. 这说明 $a\notin(x)=\mathfrak{m}$，即 a 为单位. 从而 $x^r=a^{-1}y\in\mathfrak{a}$. 于是 $\mathfrak{m}^r\subseteq\mathfrak{a}$. 但是已经有 $\mathfrak{m}^r\supseteq\mathfrak{a}$. 因此 $\mathfrak{a}=\mathfrak{m}^r=(x^r)$. 即 R 中每个理想均是主理想，从而 R 为主理想环.（并且 R 中每个理想均有形式 $\mathfrak{m}^r$.）▍

例 $\mathbf{Z}/p^n\mathbf{Z}$（p 为素数，$n\geqslant1$）和 $k[x]/(f(x)^n)$（k 为域，$f(x)$ 是 $k[x]$ 中不可约多项式）均是满足引理 28 中条件的 Artin 局部环. 因为它们的唯一极大理想分别是主理想 $(\bar{p})$ 和 $(\overline{f(x)})$.

例 设 k 为域，考虑环 $R=k[x^2,x^3]/(x^4)$. 它有合成列：$R\supset(\bar{x}^2,\bar{x}^3)\supset(\bar{x}^2)\supset0$，从而是 Artin 环. 不难验证 $U(R)=\{a_0+a_2\bar{x}^2+a_3\bar{x}^3\mid a_0,a_2,a_3\in k,a_0\neq0\}$. 而 $\mathfrak{m}=R-U(R)=(\bar{x}^2,\bar{x}^3)$ 是理想. 从而 $\mathfrak{m}$ 为 R 的唯一极大理想而 R 为局部环. 但是 $\mathfrak{m}=(\bar{x}^2,\bar{x}^3)$ 不是主理想. 或者因为 $\mathfrak{m}^2=(0)$，$R/\mathfrak{m}\cong k$，$\dim_k(\mathfrak{m}/\mathfrak{m}^2)=\dim_k\mathfrak{m}=2$，可知 Artin 局部环 $k[x^2,x^3]/(x^4)$ 不满足引理 28

中的条件。

习　题

1. M为 Artin R-模. u: $M\to M$ 是 R-模单同态. 求证 u 必为同构. [提示: 考虑一系列短正合序列 $0\to u^{n-1}(M)\xrightarrow{u}M\to M/u^n(M)\to 0$, $n=1, 2,3,\cdots$]。

2. 设 N_1 和 N_2 是 R-模M的两个R-子模, 如果 M/N_1, M/N_2 均为 Noether$R$-模, 求证 $M/(N_1\cap N_2)$ 也为 Noether R-模. 并且将"Noether"改成"Artin"这命题也是对的.

3. M 为 Artin R-模. 求证 $R/\mathrm{Ann}(M)$为 Artin 环.

4. 设 $M=M_0\supset M_1\supset\cdots\supset M_n=(0)$和 $M=M'_0\supset M'_1\supset\cdots\supset M'_n=(0)$ 是 R-模M的两个合成列.求证存在$\{1,2,\cdots,n\}$的一个置换σ,使得$M_{i-1}/M_i \cong M'_{\sigma(i)-1}/M'_{\sigma(i)}(1\leqslant i\leqslant n)$($R$-模同构). [提示: 参考群论中一类似定理的证明]。

5. (1) Abel 群A是 Noether $\mathbf{Z}$-模$\Longleftrightarrow A$是有限生成的.

(2) Abel 群A有合成列$\Longleftrightarrow A$是有限群.

6. (1) 设A为有限 Abel 群, B是A的子群. 如果$(a_1,\cdots,a_n)$ 和 $(b_1,\cdots,b_m)$分别是A和B的不变因子, 其中 $a_1|a_2|\cdots|a_n$, $b_1|b_2|\cdots|b_m$. 求证 $m\leqslant n$ 并且 $b_i|a_{i+n-m}(1\leqslant i\leqslant m)$.

(2)反之,如果$a_1|a_2|\cdots|a_n,b_1|b_2|\cdots|b_m,m\leqslant n,b_i|a_{i+n-m}(1\leqslant i\leqslant m)$ a_i,b_i 均为正整数.则存在有限 Abel 群A和它的子群B, 使得 $\{a_1,\cdots,a_n\}$ 和$\{b_1\cdots,b_m\}$分别是A和B的不变因子.

(3) 如果A是有限生成 Abel 群,那末(1)和(2) 中的结论应当改成什么样子?

7. 试问 $\mathbf{Z}/(12)\oplus\mathbf{Z}/(45)$共有多少种彼此不同构的子群?

8. 设 k 为域,$0\neq f(x)\in k[x]$. 求证 $k[x]/(f(x))$是 Artin 环. 试问如何将 $k[x]/(f(x))$表成有限个 Artin 局部环的直和?

第五章　Dedekind 整环

在这一章里，我们要介绍由 Gauss, Kummer 开创而由 Dedekind 所建立起来的 Dedekind 整环的理论．在这种整环中，每个非零理想均可唯一地表成有限个素理想之积．

Dedekind 整环是一种特殊的 Noether 整环．确切地说，就是一维 Noether 整闭整环．我们首先解释什么叫整闭，即讲述整性相关概念和环的整性扩张基本理论．然后在第 2 节研究介于 Noether 整环和 Dedekind 整环之间的一维 Noether 整环和它的局部化．这些研究对于加深对 Dedekind 整环的理解是有好处的．有了这些准备之后，我们在第 3 节讲述主要对象：Dedekind 整环的基本理论．

§ 5.1　整性相关

"整性"概念是将通常整数概念推广到一般环上的成功的尝试．

定义　设 B 为环，A 为 B 的子环．B 中元素 b 叫作**对于 A 是整的元素**，或者简称为**在 A 上整**，是指 b 是 $A[x]$ 中某个首一多项式 $f(x)=x^n+a_1x^{n-1}+\cdots+a_n(n\geqslant 1)$ 的根．换句话说，存在 $a_1,\cdots,a_n\in A, n\geqslant 1$，使得

$$b^n+a_1b^{n-1}+\cdots+a_n=0. \qquad (*)$$

这时，$(*)$ 式称作是元素 $b\in B$ 在 A 上的**整性相关方程**．

注记　(1) 如果 $b\in B$ 在环 A 上整，则以 b 为根的 $A[x]$ 中首一多项式不是唯一的，从而 b 在 A 上的整性相关方程可以有许多个．

(2) 我们称 B 中元素 b 为 A 上的**代数元素**，是指 b 是 $A[x]$ 中某个多项式 $f(x)(\deg f(x)\geqslant 1)$ 的根．显然，A 上的整元素均为

代数元素，但反之不然，因为整元素还要求 $f(x)$ 是首一多项式（见下面例 3）．但是如果 A 为域，对于 A 上的每个代数元素 b，令 $f(x)\in A[x]$，$\deg f(x)\geqslant 1$，$f(b)=0$．如果 $f(x)$ 的最高项系数为 $a\neq 0$，则 a^{-1} 属于域 A，从而 b 是首一多项式 $a^{-1}f(x)$ 的根，从而 b 也是域 A 上的整元素．这表明当 A 为域的时候，"A 上整元素"和"A 上代数元素"是一致的．

（3）由定义立刻推出，如果 A，B，C 均为环并且 $A\subseteq B\subseteq C$，则 C 中元素 c 在 A 上整 $\Rightarrow$ c 在 B 上整．

例 1 环 A 中每个元素 a 均在 A 上整．因为 a 是首一多项式 $f(x)=x-a\in A[x]$ 的根．

例 2 取 $A=\mathbf{Z}$，$B=\mathbf{Q}$（有理数域）．则 $\mathbf{Q}$ 中元素 α 在 $\mathbf{Z}$ 上整 $\Longleftrightarrow \alpha\in\mathbf{Z}$．（$\Leftarrow$ 由例 1；$\Rightarrow$ 是因为根据初等代数知道，若有理数 α 是整系数首一多项式 $f(x)\in\mathbf{Z}[x]$ 的根，则 α 必为整数．）换句话说，在 $\mathbf{Z}$ 上整的有理数即是整数．这就表明我们在一般环上定义的整性概念是通常有理整数概念的一种推广．

例 3 实数 $1/\sqrt{3}$ 在 $\mathbf{Q}$ 上整（取 $f(x)=x^2-1/3$），但是易证 $1/\sqrt{3}$ 不在 $\mathbf{Z}$ 上整，虽然 $1/\sqrt{3}$ 是 $\mathbf{Z}$ 上的代数元素（为 $3x^2-1\in\mathbf{Z}[x]$ 的根）．

设 $A\subseteq B$ 为环的扩张（这相当于说，A 和 B 均是环，而 A 是 B 的子环）．以 C 表示 B 中在 A 上整的全部元素所组成的集合．于是 $A\subseteq C\subseteq B$．人们自然要问：集合 C 上是否有好的代数结构？比如说：对于 B 中的运算，C 是否封闭？即如果 b_1 和 b_2 均是 B 中在 A 上整的元素，是否 $b_1\pm b_2$ 和 b_1b_2 也是 A 上整元素？换句话说，C 是否为 B 的子环？答案是肯定的．但是当年证明这个结果却是颇不容易的事情（$\sqrt[3]{3}$，$\sqrt[7]{5}$ 在 $\mathbf{Z}$ 上整，试设想证明 $1+\sqrt[3]{3}-\sqrt[7]{5}$ 在 $\mathbf{Z}$ 上整！）．历史上，正是为了证明这一结果，Dedekind 才创造了"模"这个重要的代数概念．现在我们沿着历史的足迹，用模来

刻画整性概念，而C为环这件事是这种刻画的自然推论.

引理 1 设$A\subseteq B$为环的扩张，$b\in B$. 则以下诸条件彼此等价：

(1) b在A上整；

(2) $A[b]$为有限生成A-模；

(3) 存在B的子环D，使得$A[b]\subseteq D$，并且D是有限生成A-模；

(4) 存在忠实$A[b]$-模M，使得M为有限生成A-模.

回忆：M叫作是忠实R-模，是指$\mathrm{Ann}\, M=\{x\in R\mid xM=(0)\}$为$R$的零理想.

证明 (1) ⇒(2)：假设$b\in B$在A上整，则有整性相关方程

$$b^n+a_1b^{n-1}+\cdots+a_n=0, a_i\in A, n\geqslant 1.$$

于是对每个$r\geqslant 0$均有$b^{n+r}=-(a_1b^{n+r-1}+\cdots+a_nb^r)$. 由此式不难归纳证明出，每个$b^m(m\geqslant 0)$均可表成$1,b,b^2,\cdots,b^{n-1}$的$A$-线性组合. 因此$A[b]$作为$A$-模是由$1,b,b^2,\cdots,b^{n-1}$生成的.

(2) ⇒(3)：取$D=A[b]$即可.

(3) ⇒(4)：取$M=D$即可. 这是忠实$A[b]$-模，因为若$y\in A[b]$，$yD=(0)$，则$y=y\cdot 1_D=0$.

(4) ⇒(1)：设$M=Au_1+\cdots+Au_m, m\geqslant 1$. 由于$bu_i\in M$，从而$bu_i=\sum_{j=1}^{m}a_{ij}u_j(a_{ij}\in A, 1\leqslant i\leqslant m)$. 这可写成矩阵形式

$$(bI_m-(a_{ij}))\begin{pmatrix}u_1\\ \vdots\\ u_m\end{pmatrix}=\begin{pmatrix}0\\ \vdots\\ 0\end{pmatrix},$$

其中I_m是m阶单位方阵. 将此式两边左乘以$bI_m-(a_{ij})$的伴

随方阵，就得到 $\det(bI_m-(a_{ij}))\cdot u_k=0(1\leqslant k\leqslant m)$. 于是 $\det(bI_m-(a_{ij}))M=(0)$. 注意 $\det(bI_m-(a_{ij}))$ 为 $A[b]$ 中元素而 M 为忠实 $A[b]$-模. 从而 $\det(bI_m-(a_{ij}))=0$. 将左边行列式展开就得到 b 在 A 上的一个整性相关方程，从而 b 在 A 上整. ▌

系 1 设 $A\subseteq B$ 为环的扩张，$b_1,\cdots,b_n\in B$ 均在 A 上整. 则环 $A[b_1,\cdots,b_n]$ 为有限生成 A-模.

证明 $n=1$ 时即为引理1. 现在对 n 归纳：令 $A_r=A[b_1,\cdots,b_r]$. 由归纳假设，A_{n-1} 为有限生成 A-模. 因为 b_n 在 A 上整，从而也在 A_{n-1} 上整. 于是 $A_n=A_{n-1}[b_n]$ 是有限生成 A_{n-1}-模，因此 A_n 也是有限生成 A-模(§ 2.1，习题10). ▌

系 2 设 $A\subseteq B$ 为环的扩张，$C=\{b\in B|b$ 在 A 上整$\}$. 则 C 为 B 的子环.

证明 设 $c,c'\in C$，则 $A[c,c']$ 为有限生成 A-模(系1). 但是 $c\pm c',cc'\in A[c,c']$，从而 $c\pm c'$ 和 cc' 均在 A 上整(引理1的(3)). 于是 $c\pm c',cc'\in C$. 这就表明 C 是 B 的子环. ▌

这样我们就证明了：如果 b 和 $b'\in B$ 均在 A 上整，则它们的和、差及乘积也在 A 上整.

定义 系2中的 C 叫作是 **A 在 B 中的整闭包**. 于是 $A\subseteq C\subseteq B$. 如果 $C=A$，则称 **A 在 B 中整闭**. 如果 $C=B$，则称 **B 在 A 上整**，并且 $A\subseteq B$ 叫作是**环的整性扩张**.

系 3 设 $A\subseteq B\subseteq C$ 是环的扩张. 如果 C 在 B 上整并且 B 在 A 上整，则 C 在 A 上整.

证明 设 $c\in C$. 则 c 在 B 上有整性相关方程

$$c^n+b_1c^{n-1}+\cdots+b_n=0,n\geqslant 1,b_i\in B.$$

令 $B'=A[b_1,\cdots,b_n]$，于是 c 也在 B' 上整，从而 $B'[c]$ 为有限生

成 B'-模．由系 1 知 B' 为有限生成 A-模，于是 $B'[c]$为有限生成 A-模，即 C 的每个元素 c 均在 A 上整．从而 C 在 A 上整．▌

系 4 设 $A\subseteq B$ 为环的扩张，C 为 A 在 B 中的整闭包．则 C 在 B 中整闭．

证明 设 $b\in B$ 在 C 上整．由于 C 在 A 上整，从而 b 在 A 上整（见系3的证明）．由 C 的定义即知 $b\in C$．这就表明 C 在 B 中整闭．▌

下一引理表明商运算和局部化运算均保持整性．

引理 2 设 $A\subseteq B$ 为环的整性扩张．

(1) 如果 $\mathfrak{b}$ 为 B 的理想，$\mathfrak{a}=\mathfrak{b}\cap A$，则 $A/\mathfrak{a}\subseteq B/\mathfrak{b}$ 为整性扩张（注意：$A/\mathfrak{a}$ 自然地看成为 $B/\mathfrak{b}$ 的子环）．

(2) 若 S 为环 A 的乘法集，则 $S^{-1}A\subseteq S^{-1}B$ 为整性扩张（注意：由算子 S^{-1} 的正合性，$S^{-1}A$ 自然地看成为 $S^{-1}B$ 的子环）．

证明 (1) 设 $b\in B$，$b^n+a_1b^{n-1}+\cdots+a_n=0(a_i\in A)$为 b 在 A 上的整性相关方程．则模 $\mathfrak{b}$ 之后，在 $B/\mathfrak{b}$ 中便有 $\bar{b}^n+\bar{a}_1\bar{b}^{n-1}+\cdots+\bar{a}_n=\bar{0}(\bar{a}_i\in A/\mathfrak{a})$．这就表明 $B/\mathfrak{b}$ 中每个元素 $\bar{b}(b\in B)$ 均在 $A/\mathfrak{a}$ 上整，即 $A/\mathfrak{a}\subseteq B/\mathfrak{b}$ 为整性扩张．

(2) 类似地，对于(1) 中 $b\in B$ 在 A 上的整性相关方程和 $s\in S$，我们有

$$(b/s)^n+(a_1/s)(b/s)^{n-1}+\cdots+a_n/s^n=0,$$

这正是元素 $b/s\in S^{-1}b$ 在 $S^{-1}A$ 上的整性相关方程．从而 $S^{-1}A\subseteq S^{-1}B$ 为整性扩张．▌

引理 2 的(2)还可推广成：

引理 3 设 $A\subseteq B$ 为环的扩张．C 为 A 在 B 中的整闭包，则对于 A 的每个乘法集 S，$S^{-1}C$ 为 $S^{-1}A$ 在 $S^{-1}B$ 中的整闭包．

证明 由引理 2 可知 $S^{-1}C$ 在 $S^{-1}A$ 上整．另一方面，如果 $b/s\in S^{-1}B(b\in B,s\in S)$在 $S^{-1}A$ 上整，则有整性相关方程

$$(b/s)^n+(a_1/s_1)(b/s)^{n-1}+\cdots+a_n/s_n=0,\quad a_i\in A,s_i\in S$$

将此等式双方乘以$(ts)^n$，$t=s_1\cdots s_n\in S$，即知$bt\in B$在A上整.于是$bt\in C$，从而$b/s=bt/st\in S^{-1}C$. 于是$S^{-1}C$为$S^{-1}A$在$S^{-1}B$中的整闭包. ▌

定义 整环R叫作是整闭的，是指R在其商域中整闭.

例如$\mathbf{Z}$是整闭整环(例2). 更一般地，每个唯一因子分解整环均是整闭整环(习题).

整环的整闭性是局部性质：

引理 4 关于整环A的下面三个条件彼此等价：

(1) A为整闭整环；

(2) 对于每个$\mathfrak{p}\in \mathrm{Spec}A$，$A_{\mathfrak{p}}$为整闭整环；

(3) 对于每个$\mathfrak{m}\in \mathrm{Max}A$，$A_{\mathfrak{m}}$为整闭整环.

证明 记K为A的商域. 由于$A_{\mathfrak{p}}\subseteq K$，从而$A_{\mathfrak{p}}$均为整环.并且$A_{\mathfrak{p}}$的商域为$K$. 令$C$为$A$在$K$中的整闭包. 由引理3知$S^{-1}C$为$A_{\mathfrak{p}}$在$K$中的整闭包($S=A-\mathfrak{p}$). 记$f$: $A\to C$为包含映射，则

A整闭$\Longleftrightarrow A=C\Longleftrightarrow f$为同构.

$A_{\mathfrak{p}}$整闭$\Longleftrightarrow A_{\mathfrak{p}}=S^{-1}C\Longleftrightarrow f_{\mathfrak{p}}:A_{\mathfrak{p}}\to S^{-1}C$为同构.

但是，f是否为环同构(即A-模同构)是局部性质. 从而由第三章引理8就可证得本引理. ▌

本节其余部分是研究环的整性扩张的基本性质.

引理 5 设$A\subseteq B$为环的整性扩张，并且B(从而A)为整环.则B为域$\Longleftrightarrow A$为域.

证明 $\Leftarrow$：对于$0\neq b\in B$，令n是b在A上的整性相关方程$b^n+a_1b^{n-1}+\cdots+a_n=0(n\geqslant 1,a_i\in A)$中最小的$n$值. 由于$B$是整环，可知$a_n\neq 0$. 如果$A$为域，则$a_n^{-1}\in A$. 从而$b^{-1}=-a_n^{-1}(b^{n-1}+a_1b^{n-2}+\cdots+a_{n-1})\in B$. 从而$B$为域.

$\Rightarrow$:对于$0 \neq a \in A$. 如果B为域，则$a^{-1} \in B$. 于是a^{-1}在A上整. 从而有整性相关方程$a^{-m} + a_1' a^{-(m-1)} + \cdots + a_m' = 0$,($m \geqslant 1, a_i' \in A$). 于是$a^{-1} = -(a_1' + \cdots + a_m' a^{m-1}) \in A$,即$A$为域.▌

系 1 设$A \subseteq B$为环的整性扩张，$\mathfrak{q} \in \mathrm{Spec}\, B$. $\mathfrak{p} = \mathfrak{q} \cap A$ ($\in \mathrm{Spec} A$). 则$\mathfrak{q} \in \mathrm{Max} B \Longleftrightarrow \mathfrak{p} \in \mathrm{Max} A$.

证明 由引理2可知$A/\mathfrak{p} \subseteq B/\mathfrak{q}$为环的整性扩张，但是$B/\mathfrak{q}$为整环,从而$B/\mathfrak{q}$为域$\Longleftrightarrow A/\mathfrak{p}$为域(引理5),这就是说$\mathfrak{q} \in \mathrm{Max} B \Longleftrightarrow \mathfrak{p} \in \mathrm{Max} A$. ▌

系 2 $A \subseteq B$为环的整性扩张,A为局部环并且$\mathfrak{m}$是A的唯一极大理想. 如果$\mathfrak{q} \in \mathrm{Spec} B$,则:$\mathfrak{q} \in \mathrm{Max} B \Longleftrightarrow \mathfrak{q} \cap A = \mathfrak{m}$.

证明 由系1直接得到,因为A只有一个极大理想$\mathfrak{m}$. ▌

系 3 设$A \subseteq B$是环的整性扩张，则限制映射$f: \mathrm{Spec} B \to \mathrm{Spec} A, \mathfrak{q} \mapsto \mathfrak{q} \cap A$为满射. 换句话说,对于每个$\mathfrak{p} \in \mathrm{Spec}\, A$，均有$\mathfrak{q} \in \mathrm{Spec} B$使得$\mathfrak{q} \cap A = \mathfrak{p}$.

证明 由引理2知道$A_\mathfrak{p} \subseteq B_\mathfrak{p}$为环的整性扩张(其中$B_\mathfrak{p} = S^{-1}B, S = A - \mathfrak{p}$). 考虑环和环同态图表

$$\begin{array}{ccc} A & \xrightarrow{i} & B \\ {\scriptstyle f_A}\downarrow & & \downarrow{\scriptstyle f_B} \\ A_\mathfrak{p} & \xrightarrow{i_\mathfrak{p}} & B_\mathfrak{p} \end{array}$$

其中i和$i_\mathfrak{p}$为包含映射，$f_A: A \to A_\mathfrak{p}$为$a \mapsto a/1$，$f_B$有类似的意义. 易知这是交换图表. 取$\mathfrak{n}$为$B_\mathfrak{p}$中任一极大理想，由系2可知$\mathfrak{n} \cap A_\mathfrak{p} = \mathfrak{p} A_\mathfrak{p}$(右边为$A_\mathfrak{p}$之唯一极大理想). 并且$f_A^{-1}(\mathfrak{p} A_\mathfrak{p}) = \mathfrak{p}$(第三章定理1的系1).令$\mathfrak{q} = f_B^{-1}(\mathfrak{n})$,则$\mathfrak{q} \in \mathrm{Spec} B$. 并且由上面的交换图表可知$\mathfrak{q} \cap A = i^{-1}(\mathfrak{q}) = i^{-1} f_B^{-1}(\mathfrak{n}) = f_A^{-1} i_\mathfrak{p}^{-1}(\mathfrak{n}) = f_A^{-1}(\mathfrak{p} A_\mathfrak{p}) = \mathfrak{p}$. ▌

系 4 设$A \subseteq B$为环的整性扩张,$\mathfrak{q}, \mathfrak{q}' \in \mathrm{Spec} B, \mathfrak{q} \subseteq \mathfrak{q}'$. 如果$\mathfrak{q} \cap A = \mathfrak{q}' \cap A$,则$\mathfrak{q} = \mathfrak{q}'$.

证明 设 $\mathfrak{p}=\mathfrak{q}\cap A=\mathfrak{q}'\cap A$，则 $\mathfrak{p}\in\operatorname{Spec}A$. 仍考虑系 3 中环的交换图表. 以 $\mathfrak{n}$ 和 $\mathfrak{n}'$ 分别表示 $\mathfrak{q}$ 和 $\mathfrak{q}'$ 在 $B_\mathfrak{p}$ 中的扩张. 则 $i_\mathfrak{p}^{-1}(\mathfrak{n})$ 和 $i_\mathfrak{p}^{-1}(\mathfrak{n}')$ 均是 $A_\mathfrak{p}$ 中素理想，并且它们在 A 中的限制均为 $\mathfrak{p}$(因为 $f_A^{-1}i_\mathfrak{p}^{-1}(\mathfrak{n})=i^{-1}f_B^{-1}(\mathfrak{n})=i^{-1}(\mathfrak{q})=\mathfrak{q}\cap A=\mathfrak{p}$，同样地 $f_A^{-1}i_\mathfrak{p}^{-1}(\mathfrak{n}')=i^{-1}f_B^{-1}(\mathfrak{n}')=i^{-1}(\mathfrak{q}')=\mathfrak{q}'\cap A=\mathfrak{p}$). 从而 $i_\mathfrak{p}^{-1}(\mathfrak{n})=i_\mathfrak{p}^{-1}(\mathfrak{n}')=\mathfrak{p}A_\mathfrak{p}\in\operatorname{Max}A_\mathfrak{p}$. 从而由系 1 可知 $\mathfrak{n}$ 和 $\mathfrak{n}'$ 均为 $B_\mathfrak{p}$ 的极大理想. 但是由 $\mathfrak{q}\subseteq\mathfrak{q}'$ 得到 $\mathfrak{n}\subseteq\mathfrak{n}'$. 从而必然 $\mathfrak{n}=\mathfrak{n}'$. 于是限制到 B 上便有 $\mathfrak{q}=\mathfrak{q}'$. ▌

定理 1 （第一提升定理） 设 $A\subseteq B$ 为环的整性扩张. $\mathfrak{p}_1$, $\mathfrak{p}_2\in\operatorname{Spec}A$, $\mathfrak{p}_1\subset\mathfrak{p}_2$. $\mathfrak{q}_1\in\operatorname{Spec}B$, $\mathfrak{q}_1\cap A=\mathfrak{p}_1$. 则存在 $\mathfrak{q}_2\in\operatorname{Spec}B$，使得 $\mathfrak{q}_2\cap A=\mathfrak{p}_2$ 并且 $\mathfrak{q}_1\subset\mathfrak{q}_2$.

证明 我们已经知道 $A/\mathfrak{p}_1\subseteq B/\mathfrak{q}_1$ 为环的整性扩张. 而$\mathfrak{p}_2$是 $A/\mathfrak{p}_1$ 中素理想. 于是有 $B/\mathfrak{q}_1$ 中素理想 Q，使得 $Q\cap A/\mathfrak{p}_1=\mathfrak{p}_2$. 但是 Q 必有形式$\mathfrak{q}_2$，其中 $\mathfrak{q}_2$ 为 B 中素理想. 于是 $\mathfrak{q}_2\supset\mathfrak{q}_1$ 并且 $\mathfrak{q}_2\cap A=\mathfrak{p}_2$. ▌

利用归纳法不难将定理 1 推广成

定理 1′ 设 $A\subseteq B$ 为环的整性扩张. $\mathfrak{p}_1\subset\mathfrak{p}_2\cdots\subset\mathfrak{p}_n$ 为 A中的素理想链，$\mathfrak{q}_1\in\operatorname{Spec}B$. $\mathfrak{q}_1\cap A=\mathfrak{p}_1$，则 B 中存在素理想链 $\mathfrak{q}_1\subset\mathfrak{q}_2\subset\cdots\subset\mathfrak{q}_n$，使得 $\mathfrak{q}_i\cap A=\mathfrak{p}_i(2\leqslant i\leqslant n)$. ▌

注记 如果定理 1 再加上一些条件，我们有另一种提升定理：

定理 2 （第二提升定理） 设 $A\subseteq B$ 为整环的整性扩张，并且 A 是整闭整环. 如果 $\mathfrak{p}_1\subset\mathfrak{p}_2\subset\cdots\subset\mathfrak{p}_n$ 是 A 中素理想链，$\mathfrak{q}_n\in\operatorname{Spec}B$, $\mathfrak{q}_n\cap A=\mathfrak{p}_n$，则存在 B 中的素理想链 $\mathfrak{q}_1\subset\mathfrak{q}_2\subset\cdots\subset\mathfrak{q}_n$ 使得 $\mathfrak{q}_i\cap A=\mathfrak{p}_i(1\leqslant i\leqslant n-1)$.

这个定理的证明要用到域论某些知识. 我们先作些准备工作.

定义 设 $A\subseteq B$ 为环的扩张，$\mathfrak{a}$ 为 A 的理想．元素 $b\in B$ 叫作是**在 $\mathfrak{a}$ 上整**，是指存在多项式 $f(x)=x^n+a_1x^{n-1}+\cdots+a_n$，$a_i\in\mathfrak{a}$，使得 $f(b)=0$．集合 $I=\{b\in B\mid b$ 在 $\mathfrak{a}$ 上整$\}$ 叫作是**$\mathfrak{a}$ 在 B 中的整闭包**．

令 C 为 A 在 B 中的整闭包，显然 $\mathfrak{a}\subseteq I\subseteq C$．下面引理给出集合 I 的一个刻画．

引理 I 设 $A\subseteq B,C,\mathfrak{a},I$ 如上所示．令 $\mathfrak{a}^e=\mathfrak{a}C$，则

$I=\sqrt{\mathfrak{a}^e}=\{c\in C\mid$ 有 $n\geqslant 1$ 使得 $c^n\in\mathfrak{a}^e\}$．从而 I 为 C 的理想．

证明 设 $b\in B$．如果 b 在 $\mathfrak{a}$ 上整，则 b 也在 A 上整，于是 $b\in C$．设 b 在 $\mathfrak{a}$ 上的整性方程为 $b^n+a_1b^{n-1}+\cdots+a_n=0$，$a_i\in\mathfrak{a}$．则 $b^n=-a_1b^{n-1}-\cdots-a_n\in\mathfrak{a}^e=\mathfrak{a}C$．因此 $b\in\sqrt{\mathfrak{a}^e}$．反之，如果 $b\in\sqrt{\mathfrak{a}^e}$，则有 $m\geqslant 1$ 使得 $b^m\in\mathfrak{a}^e$．即 $b^m=\sum\limits_{i=1}^{n}a_ic_i$，$a_i\in\mathfrak{a}$，$c_i\in C$．由于 c_i 均在 A 上整，从而 $M=A[c_1,\cdots,c_n]$ 为有限生成 A-模，并且 $b^mM\subseteq\mathfrak{a}M$．由此可证 b^m 在 $\mathfrak{a}$ 上整（请参考引理 1 中 (4) $\Rightarrow$(1) 的证明）．但是 b^m 在 $\mathfrak{a}$ 上的整性方程也可看成是 b 在 $\mathfrak{a}$ 上的整性方程．因此 b 也在 $\mathfrak{a}$ 上整．这就证明了 $I=\sqrt{\mathfrak{a}^e}$． ▮

引理 II 设 $A\subseteq B$ 为整环的扩张，并 A 是整闭的．$\mathfrak{a}$ 为 A 的理想．K 为 A 的商域．如果 $b\in B$ 在 $\mathfrak{a}$ 上整，则 b 在 K 上是代数的．又若 b 在 K 上的极小多项式为 $f(x)=x^n+a_1x^n+\cdots+a_n\in K[x]$，则 $a_i\in\sqrt{\mathfrak{a}}\,(1\leqslant i\leqslant n)$（$\sqrt{\mathfrak{a}}$ 表示 $\mathfrak{a}$ 在 A 中的根）．

证明 b 显然是 K 上的代数元素．令 L 为 b 在 K 上的分裂域．由于 b 在 $\mathfrak{a}$ 上整，从而有 $g(x)=x^m+a_1'x^{m-1}+\cdots+a_m'$，$a_i'\in\mathfrak{a}$，使得 $g(b)=0$．因为 $f(x)$ 是 b 在 K 上的极小多项式，因此 $f(x)\mid g(x)$．由于 b 在 L 中的每个 K-共轭元素 b_i 均是 $f(x)$ 的根，从而也均是 $g(x)$ 的根，即也均在 $\mathfrak{a}$ 上整．但是 a_i 是诸 b_i（即 b 的全部 K-共轭元素）的初等对称多项式．由上引理可知 a_i $(1\leqslant i\leqslant n)$

均在 $\mathfrak{a}$ 上整．但已假定 A 整闭，而$a_i \in A$，从而在上引理中取A和B分别为这里的A和K(则上引理中的C为这里的A)，于是由上引理得到$a_i \in \sqrt{\mathfrak{a}}$ $(1 \leqslant i \leqslant n)$．▌

现在证明第二提升定理．不妨设 $n=2$．与证明第一提升定理相仿．我们只需证明 $\mathfrak{p}_1$ 为分式环 $B_{\mathfrak{q}_2}$ 中某个素理想到B然后再到A的限制．根据第三章定理 1 的系2，我们只需证明 $\mathfrak{p}_1 B_{\mathfrak{q}_2} \cap A = \mathfrak{p}_1$(然后取 $\mathfrak{q}_1 = \mathfrak{p}_1 B_{\mathfrak{q}_2} \cap B$ 即可)．

设 $x \in \mathfrak{p}_1 B_{\mathfrak{q}_2}$，则 $x = y/s$，$y \in \mathfrak{p}_1 B$，$s \in B - \mathfrak{q}_2$．由引理 I 知 y在 $\mathfrak{p}_1$ 上整，由引理 II 知 y 在K(A的商域)上代数，并且若

$$y^r + u_1 y^{r-1} + \cdots + u_r = 0 \tag{1}$$

是 y 在K上的极小多项式，则 $u_i \in \sqrt{\mathfrak{p}_1} = \mathfrak{p}_1 (1 \leqslant i \leqslant r)$．如果又 $0 \neq x \in A$，则 $s = yx^{-1}$，$x^{-1} \in K$．而由(1) 式知 s 在K上的极小多项式为：

$$s^r + v_1 s^{r-1} + \cdots + v_r = 0 \quad (v_i = u_i / x^i). \tag{2}$$

于是

$$x^i v_i = u_i \in \mathfrak{p}_1 \quad (1 \leqslant i \leqslant r). \tag{3}$$

由假设B为A的整性扩张，而 $s \in B$，从而 s 在 A上整．由(2) 式和引理 II (取 $\mathfrak{a} = A$)，可知 $v_i \in \sqrt{A} = A (1 \leqslant i \leqslant r)$．如果$x \notin \mathfrak{p}_1$，由(3) 式知 $v_i \in \mathfrak{p}_1 (1 \leqslant i \leqslant r)$．再由(2) 式知 $s^r \in \mathfrak{p}_1 B \subseteq \mathfrak{p}_2 B \subseteq \mathfrak{q}_2$．这与$s \in B - \mathfrak{q}_2$ 矛盾．因此 $x \in \mathfrak{p}_1$，即 $\mathfrak{p}_1 B_{\mathfrak{q}_2} \cap A \subseteq \mathfrak{p}_1$．而 $\mathfrak{p}_1 B_{\mathfrak{q}_2} \cap A \supseteq \mathfrak{p}_1$ 是显然的．这就证明了第二提升定理．▌

习　题

1．设 $A \subseteq B$ 是环的整性扩张，Ω 为任意代数封闭域．求证每个环同态 $A \to \Omega$ 均可扩充成环同态 $B \to \Omega$．[提示：利用引理 5 系 3 和下面的域论结果：设 E/F 为域的代数扩张，Ω 为任意代数封闭域．则每个域的单同态$F \to \Omega$ 均可扩充成域的单同态 $E \to \Omega$．]

2．设 $A\subseteq B$ 为环的整性扩张，$\mathfrak{n}\in\mathrm{Max}B$，$\mathfrak{m}=\mathfrak{n}\cap A\in\mathrm{Max}A$。试问 $B_{\mathfrak{n}}$ 是否一定在 $A_{\mathfrak{m}}$ 上整？［提示：考查 $A=k[x^2-1]$，k 为域，$B=k[x]$，$\mathfrak{n}=(x-1)$，考查元素 $\frac{1}{x+1}\in B_{\mathfrak{n}}$。］

3．设 $A\subseteq B$ 为环的整性扩张．求证：

(1) $A\cap U(B)=U(A)$，

(2) $A\cap r(B)=r(A)$（$r(A)$ 表示 A 的大根）。

4．设 $A\subseteq B$ 为环的扩张，$B-A$ 对于乘法封闭．求证 A 在 B 中整闭．

5．设 $A\subseteq B$ 为整环的扩张，C 为 A 在 B 中的整闭包．$f(x)$ 和 $g(x)$ 为 $B[x]$ 中首一多项式．如果 $f(x)g(x)\in C[x]$，求证 $f(x)$ 和 $g(x)$ 均属于 $C[x]$。［提示：设 K 为 B 的商域，Ω 为 K 的代数闭包．由 $f(x)g(x)\in C[x]$ 证明 $f(x)$ 和 $g(x)$ 在 Ω 中的根均在 A 上整．于是 $f(x)$，$g(x)\in C[x]$．］

又若去掉 A 和 B 是整环的限制，则上命题仍旧成立．［提示：首先证明存在 B 的一个扩环 B'，使得 $f(x)g(x)=(x-a_1)(x-a_2)\cdots(x-a_t)$，$a_i\in B'$；然后证明与前类似．］

6．设 $A\subseteq B$ 为环的扩张，C 为 A 在 B 中的整闭包．求证 $C[x]$ 是 $A[x]$ 在 $B[x]$ 中的整闭包．［提示：设 $f(x)\in B[x]$ 在 $A[x]$ 上整．$f^m+g_1f^{m-1}+\cdots+g_m=0$，$g_i\in A[x]$．取 $r>\max\{m,\deg g_1,\cdots,\deg g_m\}$，$f_1=f-x^r$．则 $(f_1+x^r)^m+g_1(f_1+x^r)^{m-1}+\cdots+g_m=0$．这可写成：$f_1{}^m+h_1f_1{}^{m-1}+\cdots+h_m=0$，$h_m=(x^r)^m+g_1(x^r)^{m-1}+\cdots+g_m\in A[x]$．对于 $-f_1$ 和 $f_1{}^{m-1}+h_1f^{m-2}+\cdots+h_{m-1}$ 用习题5．］

7．设 R 为整环，K 为 R 的商域．对于 $0\neq a\in R$，如果 a 和 $a^{-1}\in K$ 均在 R 上整，则 $a\in U(R)$。

8．求证唯一因子分解整环必为整闭整环。

9．设 G 为环 A 的自同构群的一个有限子群。

(1) 求证 $A^G=\{a\in A|\sigma(a)=a$，对每个 $\sigma\in G\}$ 是 A 的子环，并且 A 在 A^G 上整。

(2) 设 S 为 A 的乘法集，并且 $\sigma(S)\subseteq S$（对每个 $\sigma\in G$）．则 $S^G=A^G\cap S$ 是 A^G 的乘法集，G 中每个元素均可扩充为环 $S^{-1}A$ 的自同构，并且 $(S^G)^{-1}A^G\cong(S^{-1}A)^G$（环同构）。

(3) 设 $\mathfrak{p}\in \mathrm{Spec}A^G$，$P=\{\mathfrak{q}\in \mathrm{Spec}A \mid \mathfrak{q}\cap A^G=\mathfrak{p}\}$．求证 G 在集合 P 上的作用是传递的(即对任意 $\mathfrak{q}_1,\mathfrak{q}_2\in P$，均有 $\sigma\in G$ 使得 $\sigma(\mathfrak{q}_1)=\mathfrak{q}_2$)．于是 P 为有限集．[提示：设 $a\in\mathfrak{q}$，则 $\prod\limits_{\sigma\in G}\sigma(a)\in\mathfrak{q}_1\cap A^G=\mathfrak{p}\subseteq\mathfrak{q}_2$．从而有 $\sigma\in G$ 使得 $\sigma(a)\in\mathfrak{q}_2$．由此证 $\mathfrak{q}_1\subseteq\bigcup\limits_{\sigma\in G}\sigma(\mathfrak{q}_2)$，从而有某个 $\sigma'\in G$ 使得 $\mathfrak{q}_1\subseteq\sigma'(\mathfrak{q}_2)$．于是 $\mathfrak{q}_1=\sigma'(\mathfrak{q}_2)$．]

10．设 $\{S_i \mid i\in I\}$ 和 $\{R_i \mid i\in I\}$ 为环 T 的两个子环族．并且 $S_i\subseteq R_i$，S_i 在 R_i 中整闭 (对每个 $i\in I$)．求证 $\bigcap\limits_{i\in I}S_i$ 在 $\bigcap\limits_{i\in I}R_i$ 中整闭．

11．设 $A\subseteq B$ 为环的整性扩张．求证 $\dim A=\dim B$．

12．设 $A\subseteq B$ 为环的扩张．$b\in U(B)$．求证 B 的子环 $A[b]\cap A[b^{-1}]$ 在 A 上整．

13．求证 $\mathbf{Z}[x]/(x^2+4)$ 为整环，但不是整闭整环．

§ 5.2 一维 Noether 整环，离散赋值环

设 R 为整环．我们在第四章中定义了环的维数 $\dim R$．并且由定义直接得出：

$\dim R=0\Longleftrightarrow(0)$ 为 R 的极大理想 $\Longleftrightarrow R$ 为域；

$\dim R=1\Longleftrightarrow R$ 不为域并且 R 的非零素理想均是极大理想．

本节我们研究一维 Noether 整环和一类特殊的一维 Noether 局部整环——离散赋值环．一维 Noether 整环的一个值得注意的性质是：

引理 6 一维 Noether 整环 R 的每个非零理想 $\mathfrak{a}$ 均可 (不计因子次序)唯一地表成有限个准素理想的乘积，并且这些准素理想的根两两不同．

证明 存在性：设 $\mathfrak{a}=\bigcap\limits_{i=1}^{n}\mathfrak{q}_i$，$\mathfrak{p}_i=\sqrt{\mathfrak{q}_i}$ 是 $\mathfrak{a}$ 的极小准素分解式．由 $\dim R=1$ 可知 $\mathfrak{p}_i$ 均为极大理想，从而 $\mathfrak{p}_i$ 两两不同．于是

$\mathfrak{q}_i(1\leqslant i\leqslant n)$两两互素．因此 $\mathfrak{a}=\bigcap_{i=1}^{n}\mathfrak{q}_i=\prod_{i=1}^{n}\mathfrak{q}_i$.

唯一性：如果 $\mathfrak{a}=\prod_{i=1}^{n}\mathfrak{q}_i$，$\mathfrak{q}_i$ 为 $\mathfrak{p}_i$-准素理想，并且 $\mathfrak{p}_i\ (1\leqslant i\leqslant n)$两两不同．则 $\mathfrak{p}_i$ 均是极大理想，从而 $\mathfrak{q}_i(1\leqslant i\leqslant n)$彼此互素．于是 $\mathfrak{a}=\prod_{i=1}^{n}\mathfrak{q}_i=\bigcap_{i=1}^{n}\mathfrak{q}_i$．并且右边是 $\mathfrak{a}$ 的极小准素分解式．因为 $\mathfrak{p}_i(1\leqslant i\leqslant n)$彼此不相互包含，从而每个 $\mathfrak{q}_i$ 均是 $\mathfrak{a}$ 的孤立准素分支．从而由 § 4.1 的第二唯一性定理可知$\{\mathfrak{q}_i,\cdots,\mathfrak{q}_n\}$是由 $\mathfrak{a}$ 所决定的．▌

例 主理想整环是一维 Noether 整环的典型例子．我们再举一个不是主理想整环的例子：$R=\mathbf{Z}[\sqrt{5}]$．这显然是 Noether 整环．设 $\mathfrak{p}$ 是 R 的非零素理想，$0\neq a+b\sqrt{5}\in\mathfrak{p}, a,b\in\mathbf{Z}$则 $0\neq a^2-5b^2=(a-b\sqrt{5})(a+b\sqrt{5})\in\mathfrak{p}$．于是$|R/\mathfrak{p}|\leqslant|R/(a^2-5b^2)|=|a^2-5b^2|^2<+\infty$．于是 $R/\mathfrak{p}$ 为有限整环，熟知它必然为域．从而非零素理想$\mathfrak{p}$必是极大理想．即 $\dim\mathbf{Z}[\sqrt{5}]=1$，即 $\mathbf{Z}[\sqrt{5}]$是一维 Noether 整环．但是不难证明 $\mathfrak{a}=(2,1+\sqrt{5})$不是主理想(见 § 5.3 例 7)．从而 $\mathbf{Z}[\sqrt{5}]$不是主理想整环．

一维 Noether 整环 R 对于它的素理想 $\mathfrak{p}$ 的局部化 $R_\mathfrak{p}$ 是一维 Noether 局部整环．这是由于：局部化算子保持 Noether 性，从而$R_\mathfrak{p}$为Noether局部整环．由于 $R_\mathfrak{p}$ 的素理想与R 的包含在$\mathfrak{p}$之中的素理想一一保序对应，而 $\dim R=1$，从而与 $\mathfrak{p}$ 对应的 $\mathfrak{m}=\mathfrak{p}R_\mathfrak{p}$ 就是$R_\mathfrak{p}$ 中的唯一非零素理想．因此 $\dim R_\mathfrak{p}=1$．即 $R_\mathfrak{p}$ 是一维 Noether 局部整环．我们现在介绍一类特殊的一维 Noether 局部整环，叫作是离散赋值环．首先定义什么是赋值环．

定义 设 R 为整环，K 是 R 的商域．如果对于 K 中每个非零元素 a，a 和 a^{-1} 至少有一个属于 R，则称 R 是**赋值环**．

例 1 每个域都是赋值环．

例 2 $\mathbf{Z}_{(p)}$($\mathbf{Z}$ 在素理想(p)处的局部化)，$k[x]_{(f)}$($k[x]$在素理想$(f(x))$处的局部化，其中 $k[x]$是域 k 上的多项式环，$f(x)$为 $k[x]$中不可约多项式)均是赋值环(习题 1)。

例 3 $k[[x]]$(域 R 上的形式幂级数环)为赋值环(习题 1)。

例 4 $R=\bigcup\limits_{n\geq 1} k[[x^{\frac{1}{n}}]]$($k$ 为域)是赋值环(习题 1)。

例 5 若 R 为赋值环，K 为 R 的商域，R' 为环并且 $R\subseteq R'\subseteq K$，则 R'也是赋值环。

引理 7 设 R 为赋值环，则

(1) R 为局部环；(2) R 为整闭整环。

证明 (1) 我们只需证明 $\mathrm{m}=R-U(R)$为 R 的理想。设 $a\in R, x\in \mathrm{m}$，则 $ax\in\mathrm{m}$(因为若 $ax\notin\mathrm{m}$，则 $ax\in U(R)$，从而 $x\in U(R)$，而这与 $x\in\mathrm{m}=R-U(R)$矛盾)。因此 $R\mathrm{m}\subseteq\mathrm{m}$。进而，设 $x,y\in\mathrm{m}$。如果 x 或 $y=0$，则显然 $x\pm y\in\mathrm{m}$。如果 x 和 y 均不为 0，则 $x^{-1}y$ 和 xy^{-1} 至少有一个属于 R。不妨设 $xy^{-1}\in R$。则 $x\pm y=(xy^{-1}\pm 1)y\in R\mathrm{m}\subseteq\mathrm{m}$。这就证明了 m 为 R 的理想。于是 R 为局部环。

(2) 设 $\alpha\in K$ 在 R 上整，则有整性相关方程 $\alpha^n+b_1\alpha^{n-1}+\cdots+b_n=0, b_i\in R, n\geq 1$。如果 $\alpha\in R$ 则证毕。如果 $\alpha\notin R$，则 $\alpha^{-1}\in R$。于是又得出 $\alpha=-(b_1+b_2\alpha^{-1}+\cdots+b_n\alpha^{-(n-1)})\in R$。▌

定义 域 K 上的一个**离散赋值**是指一个映射

$$\nu: K^*\longrightarrow \mathbf{Z}\quad (K^*=K-\{0\}),$$

并且满足以下两个条件：对于 $x,y\in K$，

(I) $\nu(xy)=\nu(x)+\nu(y)$，

(II) $\nu(x+y)\geq\min(\nu(x),\nu(y))$。

注记 (1) 条件(I)是说，ν 是乘法群 K^*到加法群 $\mathbf{Z}$ 中的同

态. 从而必然 $\nu(1)=0,\nu(x^{-1})=-\nu(x)$.

(2) 如果规定$\nu(0)=+\infty$，则映射扩充为$\nu:K\to\mathbf{Z}\cup\{+\infty\}$. 如果再规定 $(+\infty)+n=n+(+\infty)=(+\infty)+(+\infty)=+\infty$, $+\infty>n$(对每个整数 n),则扩充后的映射 ν 仍然满足定义中的条件(I)和(II). 今后我们恒假定 $\nu(0)=+\infty$.

(3) 不难验证:$\{x\in K\,|\,\nu(x)\geqslant 0\}$是赋值环.

定义 整环 R 叫作是**离散赋值环**,是指 R 的商域 K 存在离散赋值 ν,使得 $R=\{x\in K\,|\,\nu(x)\geqslant 0\}$.

由上面注记(3) 可知离散赋值环必然是赋值环,从而为整闭的局部整环(引理7). 我们现在要证明:离散赋值环和一维Noether 整闭局部整环是一回事. 为了今后的应用,我们还要证明一个更为细致的结果(引理 9).

引理 8 离散赋值环 R 若不为域,则必然是一维 Noether 整闭整环.

证明 只需证明 R 是 Noether 环并且 $\dim R=1$. 设 K 是 R 的商域, ν 为 K上的离散赋值, 而 $R=\{x\in K\,|\,\nu(x)\geqslant 0\}$. 由于 $\nu(K^*)$是 $\mathbf{Z}$ 的加法子群,从而 $\nu(K^*)=n\mathbf{Z}$(对某个整数 $n\geqslant 0$).如果 $n=0$, 则 $\nu(K^*)=(0)$, 而$R=K$ 为域, 这与题设不符. 从而 $n\geqslant 1$. 这时易知$\frac{1}{n}\nu:K^*\to\mathbf{Z}$, $x\mapsto\frac{1}{n}\nu(x)$也是域 K 的离散赋值. 并且对应于$\frac{1}{n}\nu$ 的离散赋值环也是 R. 由于$\frac{1}{n}\nu(K^*)=\mathbf{Z}$. 从而我们可以一开始就假定 $\nu(K^*)=\mathbf{Z}$. 于是存在 $\pi\in K^*$,使得 $\nu(\pi)=1$. 易知 $U(R)=\{x\in K\,|\,\nu(x)=0\}$, 而 R 的唯一极大理想为 $\mathfrak{m}=R-U(R)=\{x\in K\,|\,\nu(x)>0\}=\{x\in K\,|\,\nu(x)\geqslant 1\}$. 于是 $\pi\in\mathfrak{m}$,从而$(\pi)\subseteq\mathfrak{m}$. 另一方面, 对于每个 $\alpha\in\mathfrak{m},\nu(\alpha)\geqslant 1$. 从而 $\nu(\alpha/\pi)=\nu(\alpha)-\nu(\pi)\geqslant 0$. 于是 $\alpha/\pi\in R$,从而 $\alpha\in\pi R=(\pi)$, 即

$\mathfrak{m}\subseteq(\pi)$. 于是 $\mathfrak{m}=(\pi)$. 进而,设 $\mathfrak{a}$ 为 R 的任一非零理想,$l=\min\{\nu(x)\mid x\in\mathfrak{a}\}$. 则 l 为非负整数,并且有 $x\in\mathfrak{a}$ 使得 $\nu(x)=l$. 由于 $x/\pi^l\in U(R)$,从而 $\mathfrak{a}\supseteq(x)=(\pi^l)=(\pi)^l$. 而对 $\mathfrak{a}$ 中每个元素 α,均有 $\nu(\alpha)\geqslant l$. 从而 $\alpha/x\in R$. 于是 $\alpha\in(x)$,从而 $\mathfrak{a}\subseteq(x)$. 因此 $\mathfrak{a}=(x)=(\pi^l)=\mathfrak{m}^l$. 这就表明 R 是主理想整环,从而是 Noether 整环. 由于 R 中全部理想为 $\mathfrak{m}^l(l\geqslant0)$,从而 $\mathfrak{m}$ 是 R 中唯一的非零素理想. 因此 $\dim R=1$. ▌

引理 9 设 R 是一维 Noether 局部整环,$\mathfrak{m}$ 是 R 的唯一极大理想,$k=R/\mathfrak{m}$. 则下面六个条件彼此等价:

(1) R 为离散赋值环;

(2) R 为整闭整环;

(3) $\mathfrak{m}$ 为主理想;

(4) $\dim_k(\mathfrak{m}/\mathfrak{m}^2)=1$;

(5) R 的非零理想均是 $\mathfrak{m}$ 的幂;

(6) 存在 $x\in R$,使得 R 中非零理想均有形式 $(x^k)(k\geqslant0)$.

证明 在证明这个引理之前,先作两点注记.

(A) 由于在一维局部整环 R 中,$\mathfrak{m}$ 是 R 中唯一的非零素理想. 从而对于 Noether 环 R 中每个非零真理想 $\mathfrak{a}$,必然 $\sqrt{\mathfrak{a}}=\mathfrak{m}$. 但是 $\mathfrak{m}\in\operatorname{Max}R$. 从而由 § 4.2 引理 14 可知 $\mathfrak{a}$ 必然是 $\mathfrak{m}$-准素理想,并且存在 $n\geqslant1$ 使得 $\mathfrak{a}\supseteq\mathfrak{m}^n$.

(B) 由 § 4.3 引理 27 可知对每个 $n\geqslant0$ 均有 $\mathfrak{m}^n\neq\mathfrak{m}^{n+1}$.

现在证明引理 9. (1)⇒(2):由引理 8.

(2)⇒(3):设 $0\neq a\in\mathfrak{m}$. 由上面注记知道有 $n\geqslant1$ 使得 $\mathfrak{m}^n\subseteq(a)$,$\mathfrak{m}^{n-1}\nsubseteq(a)$. 于是有 $b\in\mathfrak{m}^{n-1}$,$b\notin(a)$. 令 $x=a/b\in K$(K 为 R 的商域),则 $x^{-1}\notin R$(因 $x^{-1}\in R\Rightarrow b=x^{-1}a\in(a)$). 由 R 的整闭性可知 x^{-1} 在 R 上不整. 从而 $x^{-1}\mathfrak{m}\nsubseteq\mathfrak{m}$(因若 $x^{-1}\mathfrak{m}\subseteq\mathfrak{m}$,则 $\mathfrak{m}$ 为忠实 $R[x^{-1}]$-模,并且 $\mathfrak{m}$ 为有限生成 R-模,从而由引理 1 的

(4)推得 x^{-1} 在 R 上整). 但是 $x^{-1}\mathfrak{m}=\frac{b}{a}\mathfrak{m}\subseteq R$. 从而只能 $x^{-1}\mathfrak{m}=R$. 即 $\mathfrak{m}=(x)$.

(3) ⇒(4):设 $\mathfrak{m}=(x)$,则 k-向量空间 $\mathfrak{m}/\mathfrak{m}^2$ 由 $\bar{x}$ 生成. 从而 $\dim_k(\mathfrak{m}/\mathfrak{m}^2)\leqslant 1$. 但是 $\dim_k(\mathfrak{m}/\mathfrak{m}^2)=0 \Longleftrightarrow \mathfrak{m}=\mathfrak{m}^2$. 而右边与注记(B)矛盾. 因此 $\dim_k(\mathfrak{m}/\mathfrak{m}^2)=1$.

(4)⇒(5):设 $\mathfrak{a}$ 是 R 的非零真理想. 由注记(A)知道有 $n\geqslant 1$ 使得 $\mathfrak{a}\supseteq\mathfrak{m}^n$. 但是 $R/\mathfrak{m}^n$ 为局部环,唯一极大理想是 $\overline{\mathfrak{m}}$,并且 $\overline{\mathfrak{m}}^n=(0)$. 由§4.3 中的引理 27 可知 $R/\mathfrak{m}^n$ 为 Artin 局部环. 又由于 $\dim_k(\overline{\mathfrak{m}}/\overline{\mathfrak{m}}^2)\leqslant\dim_k(\mathfrak{m}/\mathfrak{m}^2)=1$, 根据第四章引理 28 的证明可知 $\overline{\mathfrak{a}}$ 为 $\overline{\mathfrak{m}}$ 之幂. 从而 $\mathfrak{a}$ 为 $\mathfrak{m}$ 之幂.

(5)⇒(6):由注记(B)知道 $\mathfrak{m}\neq\mathfrak{m}^2$,从而有 $x\in\mathfrak{m}-\mathfrak{m}^2$. 由假设 $(x)=\mathfrak{m}^r$, 这只可能 $r=1$, 从而 $\mathfrak{m}=(x)$. 从而每个理想均为 $\mathfrak{m}^k=(x^k)$(对某个 $k\geqslant 0$).

(6)⇒(1):显然 $\mathfrak{m}=(x)$. 由注(B)知 $(x^k)\neq(x^{k+1})$. 从而对每个 $0\neq a\in R$,均有唯一的 k, 使得 $(a)=(x^k)$.定义 $\nu(a)=k$.然后对于 $a/b\in K^*$(K 为 R的商域,$a,b\in R$),定义$\nu(a/b)=\nu(a)-\nu(b)$. 直接验证如此定义了函数 $\nu:K^*\to\mathbf{Z}$, 并且 ν 是K的离散赋值,而$R=\{x\in K\mid\nu(x)\geqslant 0\}$. ▍

例 6 现在我们重新考查例 1 到例 4 给出的赋值环. 对于任意域K, 定义 $\nu:K^*\to\mathbf{Z}$ 为取值恒为 0 的函数, 而 $\nu(0)=+\infty$.可直接验证这是域K的离散赋值(通常称作是域K的平凡赋值). 而K是K对此离散赋值的离散赋值环. 这就表明每个域均为离散赋值环.

考查有理数域Q. 如果 $0\neq n\in\mathbf{Z}, n=\pm p^t n'$, 其中 p 为固定的素数,而$(p,n')=1$.我们定义 $\nu_p(n)=t$. 而对 $0\neq a/b\in\mathbf{Q}$, a, $b\in\mathbf{Z}$,定义 $\nu_p(a/b)=\nu_p(a)-\nu_p(b)$. 直接验证 ν_p 是域 Q 的离散

赋值，并且 $\mathbf{Z}_{(p)}=\left\{\frac{a}{b}\in \mathbf{Q}\ \middle|\ a,b\in \mathbf{Z},b\neq 0,(p,b)=1\right\}=\{a\in \mathbf{Q}\mid \nu_p(a)\geqslant 0\}$. 这就表明 $\mathbf{Z}_{(p)}$是离散赋值环. ν_p 通常称作是 p-adic 指数赋值. 它是代数数论中经常使用的工具.

设 k 为域，$f(x)$是 $k[x]$中不可约多项式. 由于 $k[x]$是主理想整环，从而 $k[x]$ 中每个多项式均可写成 $g(x)=f(x)^t h(x)$，$t\geqslant 0,(h,f)=1$. 定义 $\nu_f(g(x))=t$. 而 $\nu_f\left(\frac{g(x)}{g'(x)}\right)=\nu_f(g)-\nu_f(g')$. 则 ν_f 为有理函数域 $k(x)$ 的离散赋值. 并且 $k[x]_{(f)}$ 是对应的离散赋值环.

对于形式幂级数环 $k[[x]]$，以 $k((x))$ 表示它的商域. 我们知道，$f(x)=a_0+a_1x+\cdots+a_nx^n+\cdots(\in k[[x]])$为$k[[x]]$中单位$\Longleftrightarrow a_0\neq 0$. 于是 $k[[x]]$ 中非零元素均可唯一表成 $f(x)=x^t\cdot f_0(x)$，$f_0(x)$ 为 $k[[x]]$中单位. 定义 $\nu_x(f(x))=t$. 然后将 ν_x扩充到域 $k((x))$ 之上. 即知 ν_x 是 $k((x))$ 的离散赋值. 而 $k[[x]]$是对应的离散赋值环.

最后我们考虑例 4 中的赋值环$R=\bigcup\limits_{n\geqslant 1}k[[x^{\frac{1}{n}}]]$. 可直接验证它的唯一极大理想为 $\mathfrak{m}=\{f(x)\in R\mid f(x)\text{常数项为 }0\}$. 它是由集合$\{x^{\frac{1}{n}}\mid n\geqslant 1\}$或者集合 $\{x^{\frac{1}{p}}\mid p\text{ 为素数}\}$生成的理想. 这不是主理想. 从而由引理 9 可知R不是离散赋值环.

例 7 以引理 9 为背景，现在我们构作一个不是离散赋值环的一维 Noether 局部整环. 我们在引理 6 的后面给出例子 $R=\mathbf{Z}[\sqrt{5}]$，它是一维Noether整环. 考虑R的理想$\mathfrak{p}=(2,1+\sqrt{5})$. 由于$R/\mathfrak{p}$只有两个元素$\bar{0}$和$\bar{1}$从而 $\mathfrak{p}$ 为 R 的极大理想，而 $R_\mathfrak{p}$ 为一维 Noether 局部整环. 但是 $R_\mathfrak{p}$ 不整闭，因为R和 $R_\mathfrak{p}$ 的商域均为二次域 $\mathbf{Q}[\sqrt{5}]$，而 $\mathbf{Q}[\sqrt{5}]$中元素$\frac{1}{2}(1+\sqrt{5})$在 $R_\mathfrak{p}$上整 $\Big(\frac{1}{2}$

$(1+\sqrt{5})$为 $f(x)=x^2-x-1$ 的根). 由于$\frac{1}{2}(1+\sqrt{5})\notin R_p$. 从而$R_p$不整闭. 于是由引理 9 知 R_p 不是离散赋值环.

习 题

1. 直接验证例 2 到例 4 均是赋值环.

2. 设 A 为域 K 的子环, $\bar{A}$ 为 A 在 K 中的整闭包, 求证 $\bar{A}=\cap\{K$ 的赋值环 $B \mid B\supseteq A\}$.

3. 设 R 为赋值环但不为域. 求证: R 为离散赋值环$\Longleftrightarrow R$ 为 Noether 环.

4. 设 R 为局部整环且不为域, R的唯一极大理想 $\mathfrak{m}$ 是主理想, 并且 $\bigcap\limits_{n\geqslant 1}\mathfrak{m}^n=(0)$. 求证 R 是离散赋值环.

5. 设 K 为域, Ω 为任意代数封闭域. 定义集合

$\Sigma=\{(A,f)\mid A$ 为K 的子环, $f:A\to\Omega$ 为环同态$\}$.

在Σ上定义关系

$(A,f)\leqslant(A',f')\Longleftrightarrow A\subseteq A'$ 并且$f'|_A=f$.

(1) 求证 $(\Sigma,\leqslant)$ 是部分序集合, 并且 $(\Sigma,\leqslant)$ 至少有一个极大元.

(2) 设 (B,g) 为 $(\Sigma,\leqslant)$ 的一个极大元, 则 B 为局部环, 并且 $\mathfrak{m}=\mathrm{Ker}\,g$ 是它的唯一极大理想.

(3) 对于每个 $0\neq\alpha\in K$, 则或者 $\mathfrak{m}[\alpha]\neq B[\alpha]$, 或者 $\mathfrak{m}[\alpha^{-1}]\neq B[\alpha^{-1}]$.

(4) B 为域 K 的赋值环. [提示: 对 $0\neq\alpha\in K$. 如果 $\mathfrak{m}[\alpha]\neq B(\alpha)$, 我们证 $\alpha\in B$: 由假设 $\mathfrak{m}[\alpha]$ 包含在环 $B'=B[\alpha]$的某个极大理想 $\mathfrak{m}'$ 之中. 证明 $\mathfrak{m}'\cap B=\mathfrak{m}$. 由包含映射诱导出域的单同态 $k=B/\mathfrak{m}\to k'=B'/\mathfrak{m}'$, 并且 $k'=k[\bar{\alpha}]$. 证明 k'/k 为域的有限扩张. 由于 $\mathfrak{m}=\mathrm{Ker}\,g$, 从 $g:B\to\Omega$ 诱导出域的单同态 $\bar{g}:k=B/\mathfrak{m}\to\Omega$. 然后又扩充成域的单同态 $\bar{g}:k'\to\Omega$. 它与自然同态 $B'\to k'=B'/\mathfrak{m}'$ 合成出 $g':B'\to\Omega$. 验证 $g'|B=g$. 于是由 (B,g) 的极大性推知 $B=B'$. 即 $\alpha\in B$. 类似地由 $\mathfrak{m}[\alpha^{-1}]\neq B[\alpha^{-1}]$ 得到 $\alpha^{-1}\in B$. 由 (3) 即知 B 为 K 的赋值环.]

6. 设 R 为整环, 则: R 为赋值环 $\Longleftrightarrow R$ 为局部环并且 R 的每个有限生成理想均是主理想.

§ 5.3 Dedekind 整环

现在谈本章的主题.

定义 一维 Noether 整闭整环叫作是 Dedekind 整环.

换句话说,一个整环 R 是 Dedekind 整环,是指它满足三个条件:

(1) $\dim R=1$;即 R 不是域并且非零素理想均是极大理想.

(2) R 在它的商域 K 中整闭;

(3) R 为 Noether 环.

这三个条件都是不可缺少的. 例如:

例 1 我们在上一节中给出的 $R=\mathbf{Z}[\sqrt{5}]$是一维 Noether 整环,但不整闭 ($\frac{1}{2}(1+\sqrt{5})$ 在 R 上整但不属于 R).

例 2 对于任意域 k, $R=k[x_1, x_2]$ 为 Noether 整环 (Hilbert 基定理). 由于 $k[x_1,x_2]$ 为唯一因子分解整环,从而是整闭整环. 但是有长为 2 的素理想链 $0\subset(x_1)\subset(x_1,x_2)$. 从而 $\dim R\geqslant 2$ (事实上我们在第七章将证明 $\dim R=2$).

例 3 上一节中给出的赋值环 $R=\bigcup\limits_{n\geq 1}k[[x^{\frac{1}{n}}]]$ 为整闭局部整环. R 中每个元素均可唯一地表达成 $f(x)=x^{\alpha}f_0(x)$,其中 α 为非负有理数,而 $f_0(x)\in U(R)$ (即 $f_0(x)$ 的常数项不为0). 如果我们定义 $\nu_x: R\to\mathbf{Q}$, $\nu_x(f)=\alpha$. 可知 R 的唯一极大理想即为 $\mathfrak{m}=\{f(x)\in R\,|\,\nu_x(f)>0\}$. 对 R 中每个真理想 $\mathfrak{a}$, 均有 $\mathfrak{a}\subseteq\mathfrak{m}$. 如果 $\mathfrak{a}\neq\mathfrak{m}$,则必存在正实数 α, 使得 $\mathfrak{a}=\{f(x)\in R\,|\,\nu_x(f)\geqslant\alpha\}$ 或者 $\mathfrak{a}=\{f(x)\in R\,|\,\nu_x(f)>\alpha\}$. 这样的 $\mathfrak{a}$ 显然不是素理想. 因此 $\mathfrak{m}$ 是 R 中唯一的非零素理想. 于是 $\dim R=1$. 但是 R 不为 Noether 环,因为 $\mathfrak{m}$ 不是有限生成理想.

本节中我们首先讲 Dedekind 整环的一些重要性质和刻画

Dedekind 整环的各种方式，然后给出 Dedekind 整环上有限生成模的结构和分类，最后讲一个重要的定理（定理 11）和类群问题.

先谈第一个问题. 通过前两节的准备工作，我们首先得到如下的结果.

定理 4 设 R 为一维 Noether 整环，则下列三条件彼此等价：

(1) R 为 Dedekind 整环；

(2) R 中准素理想均为素理想的幂；

(3) 对于每个 $(0)\neq\mathfrak{p}\in\operatorname{Spec}R$，$R_\mathfrak{p}$ 均为离散赋值环.

证明 (1)$\Longleftrightarrow$(3)： 在定理 4 的假定之下，则

(1)$\Longleftrightarrow R$ 整闭$\Longleftrightarrow$对每个 $(0)\neq\mathfrak{p}\in\operatorname{Spec}R$，$R_\mathfrak{p}$ 整闭（引理 4）

$\Longleftrightarrow$(3)（引理 9，因为 $R_\mathfrak{p}$ 为一维 Noether 局部整环）.

(3)$\Longleftrightarrow$(2)：类似地我们有

(3)$\Longleftrightarrow$对每个 $(0)\neq\mathfrak{p}\in\operatorname{Spec}R$，$R_\mathfrak{p}$ 中非零理想均为 $\mathfrak{p}R_\mathfrak{p}$ 之幂（引理 9）

$\Longleftrightarrow$对每个 $(0)\neq\mathfrak{p}\in\operatorname{Spec}R$，$R$ 中 $\mathfrak{p}$-准素理想均为 $\mathfrak{p}$ 之幂

$\Longleftrightarrow$(2). ▌

注记 由于引理 9，我们还可以在定理 4 中再加上一些等价的条件，如

(4) 对于每个 $(0)\neq\mathfrak{p}\in\operatorname{Spec}R$，$\mathfrak{p}R_\mathfrak{p}$ 为 $R_\mathfrak{p}$ 的主理想；

(5) 对于每个 $(0)\neq\mathfrak{p}\in\operatorname{Spec}R$，$\dim_k(\mathfrak{m}/\mathfrak{m}^2)=1$ $(\mathfrak{m}=\mathfrak{p}R_\mathfrak{p}, k=R_\mathfrak{p}/\mathfrak{m})$ 等等.

由引理 6，一维 Noether 整环中每个非零理想均可唯一地表成有限个准素理想之积. 而由定理 4 我们又知道在 Dedekind 整环 R 中，每个 $\mathfrak{p}$-准素理想 $\mathfrak{q}$ 均有形式 $\mathfrak{p}^n$. 考虑 R 和 $R_\mathfrak{p}$ 中理想

之对应关系，可知当 $n \neq n'$ 时，$\mathfrak{p}^n \neq \mathfrak{p}^{n'}$. 于是我们得到 Dedekind 整环中一个非常重要的性质：

系 1 在 Dedekind 整环中，每个非零理想（不计因子次序）均可唯一地表示成有限个素理想之积. ▌

从现在起，我们谈 Dedekind 整环 R 中的理想均指非零理想. 以 $I_0(R)$ 表示 R 中（非零）理想全体对理想乘法组成的半群. 系 1 表明，它是以 $\mathrm{Spec}R-\{0\}$ 为基的自由交换幺半群. 幺元素为理想 $(1)=R$. 熟知这样的半群中是有消去律的，也就是说我们有

系 2 设 $\mathfrak{a},\mathfrak{b},\mathfrak{c}$ 为 Dedekind 整环 R 中的理想. 如果 $\mathfrak{ac}=\mathfrak{bc}$，则 $\mathfrak{a}=\mathfrak{b}$. ▌

具有消去律的交换幺半群 M 均可扩充成交换群 G，使得 G 中元素均可表成 M 中两个元素之商. 其作法和整环扩充成商域的过程是一样的. 但是对于目前我们 $M=I_0(R)$ 这一具体情形，G 中元素不仅为形式化的等价类 a/b $(a, b\in M)$，还可以赋以更具体的意义，这就是所谓"分式理想"概念. 这个概念对于任何整环 R 都是可以定义的.

定义 设 R 为任意整环，K 是它的商域. 设 M 是 R-模 K 的 R-子模，$M\neq(0)$，并且存在元素 $0\neq a\in R$ 使得 $aM\subseteq R$. 我们便称 M 是 R 的一个**分式理想**. 换句话说，R 的分式理想 M 是商域 K 中的一个非零集合，M 为 R-模，并且 M 中全体元素表成 R 中两个元素之商时可以有一个"公分母" a. 这时，aM 为 R 的 R-子模，从而 aM 就是 R 的理想.

例 4 R 中每个理想 $\mathfrak{a}$ 均是 R 的分式理想. 因为可取 $a=1$. 今后为明确起见，R 中的理想称作是**整理想**，以别于更一般的分式理想.

例 5 对于每个元素 $0\neq\alpha\in K$，$(\alpha)=\alpha R$ 为 R 的分式理想. 因为 αR 显然是 R-模，并且若 $\alpha=\frac{a}{b}$，$a,b\in R$，$b\neq 0$，则 b 就是 αR 的一个公分母：$b\cdot\alpha R=aR\subseteq R$. 我们称这种分式理想 $(\alpha)=\alpha R$ $(0\neq\alpha\in K)$ 为由 α 生成的**主分式理想**. 当 $0\neq\alpha\in R$ 时，(α) 即是主整理想.

例 6 更一般地，K 的每个有限生成 R-子模 M 均是分式理想. 因为若 $M=R\alpha_1+\cdots+R\alpha_n$，$0\neq\alpha_i\in K$ $(1\leqslant i\leqslant n)$. 以 b 表示 $\alpha_1,\cdots,\alpha_n$ 的一个公分母（如取 b 为 $\alpha_1,\cdots,\alpha_n$ 的分母之积），则 $b\alpha_i\in R$ $(1\leqslant i\leqslant n)$，从而 $bM=Rb\alpha_1+\cdots+Rb\alpha_n\subseteq R$. 反过来，如果 R 是Noether 整环，则 R 的每个分式理想 M 也必然是 K 的有限生成 R-子模. 因为若 $bM\subseteq R$ $(0\neq b\in R)$，则 bM 是 R 的整理想. 当 R 为Noether 环时，bM 是有限生成的，即 $bM=Ra_1+\cdots+Ra_n$ $(a_i\in R)$. 于是 $M=Ra_1/b+\cdots+Ra_n/b$，即 M 是 K 的有限生成 R-子模. 所以在 R 为 Noether 整环的时候，"R 的分式理想"和"K 的有限生成 R-子模"这两个概念是一致的.

现在仍设 R 是任意的整环，K 为它的商域. 任意两个 R-模通常是不能定义乘法的. 但是如果 M 和 N 是 K 的两个 R-子模. 由于 M 和 N 为 K 的子集合而域 K 中有乘法，我们可以定义 M 和 N 的乘积为

$$MN=\{\sum_{i=1}^{l}m_in_i\,|\,m_i\in M,n_i\in N,l\geqslant 1\}.$$

不难验证 MN 仍是 K 的 R-子模. 如果 M 和 N 是 R 的分式理想，则 MN 也是 R 的分式理想（若 α 和 β 分别为 M 和 N 的公分母，则 $\alpha\beta$ 为 MN 的公分母）. 从而，若以 $I(R)$ 表示全体 R 的分式理想组成的集合，则 $I(R)$ 对于上述定义的乘法形成交换幺半群，幺元素为 $(1)=R$.

什么是幺半群 $I(R)$ 中的单位（即乘法可逆元素）？

定义 K 的 R-子模 M 叫作是**可逆理想**，是指存在 K 的 R-子模 N，使得 $MN=R$.

注记 (1) 如果 M 是可逆理想，则满足 $MN=R$ 的 K 中的 R-子模 N 当然也是可逆理想，并且由于

$$N\subseteq(R:M)=(R:M)R=(R:M)MN\subseteq RN=N.$$

从而 $N=(R:M)$. 换句话说，如果 M 是可逆理想，则 N 是唯一决定的. 我们称 N 为 M 的逆，记为 $N=M^{-1}$. 于是 $M^{-1}=(R:M)$.

(2) 可逆理想 M 必然是 R-分式理想. 因为由 $MN=R$ 可知存在 $x_i\in M, y_i\in N$ $(1\leqslant i\leqslant n)$ 使得 $1=\sum_{i=1}^{n}x_iy_i$. 从而对每个 $x\in M$, $x=\sum_{i=1}^{n}(y_ix)x_i$, $y_ix\in MN=R$. 于是 M 是由 $x_1,\cdots,x_n$ 生成的 R-模. 由例 6 所述可知 M 是 R 的分式理想.

(3) 回到原来的问题，我们现在可以说：M 是半群 $I(R)$ 中的可逆元 $\Longleftrightarrow$ M 是可逆理想. 从而，$I(R)$ 为群 $\Longleftrightarrow$ 每个 R 的分式理想均是可逆理想. 我们下一个目标是要证明：这又恰好等价于 R 是 Dedekind 整环！为了证明这一点，我们首先证明 R 的分式理想的可逆性是局部性质，然后再利用局部结果.

引理10 设 M 为整环 R 的分式理想，则下列三条件彼此等价：

(1) M 为可逆理想；

(2) M 为有限生成 R-模，并且对每个 $(0)\neq\mathfrak{p}\in\operatorname{Spec}R$，分式模 $M_\mathfrak{p}$ 均可逆（注意：$M_\mathfrak{p}$ 是 K 的 $R_\mathfrak{p}$-子模，而 $R_\mathfrak{p}$ 为整环）.

(3) M 为有限生成 R-模，并且对每个 $(0)\neq\mathfrak{m}\in\operatorname{Max}R$,

$M_{\mathfrak{m}}$ 均可逆.

证明 (1)⇒(2):由前面注记 (2) 知可逆理想 M 是有限生成 R-模. 并且 $M(R:M)=R$. 作用良好的局部化算子,得到 $M_{\mathfrak{p}}(R_{\mathfrak{p}}:M_{\mathfrak{p}})=R_{\mathfrak{p}}$. 从而 $M_{\mathfrak{p}}$ 作为 $R_{\mathfrak{p}}$-模是可逆的.

(2)⇒(3):显然成立.

(3)⇒(1):令 $\mathfrak{a}=M(R:M)$,这是 R 的整理想. 根据假设,对每个 $(0)\neq\mathfrak{m}\in \mathrm{Max}R$,均有 $R_{\mathfrak{m}}=M_{\mathfrak{m}}(R_{\mathfrak{m}}:M_{\mathfrak{m}})=\mathfrak{a}_{\mathfrak{m}}$. (这里用到了 M 为有限生成 R-模,从而 $M_{\mathfrak{m}}$ 为有限生成 $R_{\mathfrak{m}}$-模.)从而 $\mathfrak{a}$ 不包含在任何极大理想之中(因若 $\mathfrak{a}\subseteq\mathfrak{m}$, 则 $\mathfrak{a}_{\mathfrak{m}}$ 为 $R_{\mathfrak{m}}$ 的真理想). 于是 $\mathfrak{a}=R$,即 $R=M(R:M)$. 这表明 M 是可逆理想. ▌

引理 10 把问题归结为局部情形,而对局部情形恰好有:

引理 11 设 R 为局部整环,则: R 的每个分式理想均可逆 $\Longleftrightarrow R$ 为离散赋值环.

证明 ⇐:我们在引理 8 的证明中给出离散赋值环 R 的良好结构:它的极大理想是主理想 $\mathfrak{m}=(x)$,并且 R 中每个整理想均有形式 $(x^r)(r\geq 0)$. 设 M 为 R 的分式理想,则有 $0\neq a\in R$ 使得 aM 为整理想. 令 $aM=(x^r)$,则$(a)M=(x^r)$. 从而(ax^{-r})就是 M 之逆. 即 R 的分式理想均可逆.

⇒:由于 R 的整理想均为分式理想.由假设它们均可逆,从而是有限生成的.于是R是Noether 局部整环.根据 §4.3 的引理27, Noether 局部环 R 有两种情形: $\mathfrak{m}^n=(0)$是不可能的(因为R是整环),因此有 $R\supset\mathfrak{m}\supset\mathfrak{m}^2\supset\cdots\supset\mathfrak{m}^n\supset\cdots$. 令 $\mathfrak{m}^\infty=\bigcap_{n=0}^{\infty}\mathfrak{m}^n$,这是 R 的理想并且 $\mathfrak{m}\mathfrak{m}^\infty=\mathfrak{m}^\infty$(显然 $\mathfrak{m}\mathfrak{m}^\infty\subseteq\mathfrak{m}^\infty$. 反之若 $x\in\mathfrak{m}^\infty$,则对每个 $n\geq 0$,$(x)\subseteq\mathfrak{m}^n$. 由于 $\mathfrak{m}$ 可逆从而 $\mathfrak{m}^{-1}(x)\subseteq\mathfrak{m}^{n-1}$. 于是 $\mathfrak{m}^{-1}(x)\subseteq\mathfrak{m}^\infty$,即$(x)\subseteq\mathfrak{m}\cdot\mathfrak{m}^\infty$. 从而 $\mathfrak{m}^\infty\subseteq\mathfrak{m}\cdot\mathfrak{m}^\infty$). 由中山引理可知

$\mathfrak{m}^{n}=(0)$. 于是对 R 中每个理想 $\mathfrak{a}\neq(0)$，必有 $n\geqslant1$, 使得 $\mathfrak{a}\nsubseteq\mathfrak{m}^{n}$, $\mathfrak{a}\subseteq\mathfrak{m}^{n-1}$. 于是 $\mathfrak{a}\cdot\mathfrak{m}^{-(n-1)}\nsubseteq\mathfrak{m}$, $\mathfrak{a}\cdot\mathfrak{m}^{-(n-1)}\subseteq R$. 这就表明 $\mathfrak{a}\cdot\mathfrak{m}^{-(n-1)}=R$. 于是 $\mathfrak{a}=\mathfrak{m}^{n-1}$. 从而 R 中每个非零理想均可写成 $\mathfrak{m}$ 之幂. 于是 $\dim R=1$. 再由引理 9 即知 R 是离散赋值环. ▌

回到整体上来我们就得到

定理 5 设 R 为整环，则 R 为 Dedekind 整环 $\Longleftrightarrow R$ 的每个分式理想均可逆.

证明 $\Rightarrow$: 若 M 为 R 的分式理想, 则对每个 $(0)\neq\mathfrak{p}\in\operatorname{Spec}R$, $M_{\mathfrak{p}}$ 是 $R_{\mathfrak{p}}$ 的分式理想. $R_{\mathfrak{p}}$ 为离散赋值环 (定理 4), 从而 $M_{\mathfrak{p}}$ 可逆 (引理 11). 又因为 R 为Noether 环, 可知 M 是有限生成 R-模. 于是由引理 10 即知 M 为可逆的.

$\Leftarrow$: R 的整理想均可逆, 从而均是有限生成的, 这表明 R 为 Noether 整环. 对于每个 $(0)\neq\mathfrak{p}\in\operatorname{Spec}R$. 令 $\mathfrak{b}$ 为 $R_{\mathfrak{p}}$ 的非零整理想, 则 $\mathfrak{a}=\mathfrak{b}\cap R$ 是 R 中可逆理想. 由引理 10 知 $\mathfrak{b}=\mathfrak{a}_{\mathfrak{p}}$ 为 $R_{\mathfrak{p}}$ 中可逆理想. 于是 $R_{\mathfrak{p}}$ 为离散赋值环(引理 11, 注意: $R_{\mathfrak{p}}$ 的每个非零整理想均可逆, 则每个分式理想也必可逆). 最后, 由于 $\mathfrak{p}R_{\mathfrak{p}}$ 是 $R_{\mathfrak{p}}$ 中的唯一非零素理想, 从而 R 的每个非零素理想都不会包含在另一个素理想之中. 因此 $\dim R=1$. 再由定理 4 即知 R 为 Dedekind 整环. ▌

由定理 5 和引理 10 之前的注记(3), 立刻得到:

系 1 设 R 为整环, 则: R 为 Dedekind 整环 $\Longleftrightarrow R$ 的分式理想集合 $I(R)$ 为乘法群. ▌

系 2 设 R 为整环, 则: R 为 Dedekind 整环 $\Longleftrightarrow R$ 的每个非零整理想均可表成有限个素理想之积.

证明 $\Rightarrow$: 由定理 4 的系 1.

$\Leftarrow$: 根据系 1, 我们只需证明 R 的每个非零素理想 $\mathfrak{p}$ 均可逆. 设 $0\neq c\in\mathfrak{p}$, 则 $(c)\subseteq\mathfrak{p}$. 将理想 (c) 表成素理想乘积则 $(c)=\mathfrak{p}_1\cdots$

$\mathfrak{p}_k\subseteq\mathfrak{p}$. 从而有某个 $i(1\leqslant i\leqslant k)$使得 $\mathfrak{p}_i\subseteq\mathfrak{p}$. 由于(c)可逆，因此 $\mathfrak{p}_i$ 也可逆. 我们只需再证可逆素理想 $\mathfrak{p}_i$ 必为极大理想，因为这时由 $\mathfrak{p}_i\subseteq\mathfrak{p}$ 推得 $\mathfrak{p}_i=\mathfrak{p}$，于是 $\mathfrak{p}$ 为可逆理想，从而证得系 2.

现在证明可逆素理想 $\mathfrak{p}_i$ 必为极大理想：如果 $\mathfrak{p}_i$ 不是极大理想，则有极大理想 $\mathfrak{m}$ 使得 $\mathfrak{m}\supset\mathfrak{p}_i$. 取 $a\in\mathfrak{m}-\mathfrak{p}_i$. 则 $\mathfrak{p}_i+Ra$ 和 $\mathfrak{p}_i+Ra^2$ 都是 R 的真理想. 从而有素理想分解式：

$$\mathfrak{p}_i+Ra=P_1\cdots P_m,\quad \mathfrak{p}_i+Ra^2=Q_1\cdots Q_n. \tag{1}$$

在整环 $R/\mathfrak{p}_i$ 中，它们变成：$(\bar{a})=\bar{P}_1\cdots\bar{P}_m$，$(\bar{a})^2=\bar{Q}_1\cdots\bar{Q}_n$. 其中 $\bar{P}_i,\bar{Q}_j$ 为 $R/\mathfrak{p}_i$ 中的素理想. 由于主理想$(\bar{a})$和$(\bar{a}^2)$可逆，从而 $\bar{P}_i,\bar{Q}_j$ 也是 $R/\mathfrak{p}_i$ 的可逆理想. 并且 $\bar{P}_1{}^2\cdots\bar{P}^2{}_m=\bar{Q}_1\cdots\bar{Q}_n$. 不妨设 $\bar{P}_1$ 是集合$\{\bar{P}_1,\cdots,\bar{P}_m\}$中的极小元. 由于 $\bar{P}_1\supseteq\bar{Q}_1\cdots\bar{Q}_n$，从而 $\bar{P}_1\supseteq\bar{Q}_j$(对某个 j)，同样有 $\bar{Q}_j\supseteq\bar{P}_i$ (对某个 i)，于是 $\bar{P}_1\supseteq\bar{Q}_j\supseteq\bar{P}_i$，但是由 $\bar{P}_1$ 的极小性可知 $\bar{P}_1=\bar{P}_i$，从而 $\bar{P}_1=\bar{Q}_j$. 由于 $\bar{P}_1$ 是可逆理想，在 $\bar{P}_1{}^2\cdots\bar{P}^2{}_m=\bar{Q}_1\cdots\bar{Q}_n$ 式两边乘以 $\bar{P}_1{}^{-1}$ 之后，便去掉一个素因子. 如此继续下去，我们便可证得 $n=2m$，并且适当改变 $\bar{Q}_j$ 的下标，可使得 $\bar{P}_i=\bar{Q}_{2i-1}=\bar{Q}_{2i}(1\leqslant i\leqslant m)$. 回到 R 中便有 $P_i=Q_{2i-1}=Q_{2i}$. 于是由(1)式得到 $\mathfrak{p}_i+Ra^2=(\mathfrak{p}_i+Ra)^2$，从而 $\mathfrak{p}_i\subset\mathfrak{p}_i+Ra^2=(\mathfrak{p}_i+Ra)^2\subseteq\mathfrak{p}_i{}^2+Ra$. 由此推得 $\mathfrak{p}_i=\mathfrak{p}_i{}^2+\mathfrak{p}_ia$($\mathfrak{p}_i\supseteq\mathfrak{p}_i^2+\mathfrak{p}_ia$ 显然. 反之对 $b\in\mathfrak{p}_i$ 则 $b\in\mathfrak{p}_i^2+Ra$. 于是 $b=s+ra$，$s\in\mathfrak{p}_i^2$，$r\in R$. 于是 $ra=b-s\in\mathfrak{p}_i$. 由于 $a\notin\mathfrak{p}_i$，从而 $r\in\mathfrak{p}_i$. 于是 $b\in\mathfrak{p}_i^2+\mathfrak{p}_ia$. 即 $\mathfrak{p}_i\subseteq\mathfrak{p}_i^2+\mathfrak{p}_ia$). 这就是说 $\mathfrak{p}_i=\mathfrak{p}_i(\mathfrak{p}_i+Ra)$. 但是 $\mathfrak{p}_i$ 可逆，从而 $R=\mathfrak{p}_i+Ra\subseteq\mathfrak{m}$. 这就导致矛盾. 于是 $\mathfrak{p}_i$ 必为极大理想. 因而也就完成了系 2 的证明. ∎

定义 设 $\mathfrak{a}$ 和 $\mathfrak{b}$ 是环 R 的两个非零理想. 如果有 R 的理想 $\mathfrak{c}$ 使得 $\mathfrak{a}\mathfrak{c}=\mathfrak{b}$，则称 $\mathfrak{a}$ **整除** $\mathfrak{b}$，并表示成 $\mathfrak{a}|\mathfrak{b}$.

系 3 设 R 是 Dedekind 整环. 非零整理想 $\mathfrak{a}$ 和 $\mathfrak{b}$ 的素理想分解式为

$$\mathfrak{a}=\mathfrak{p}^{\alpha_1}\cdots\mathfrak{p}_s^{\alpha_s},\quad \mathfrak{b}=\mathfrak{p}_1^{\beta_1}\cdots\mathfrak{p}_s^{\beta_s},$$

其中 $\mathfrak{p}_1,\cdots,\mathfrak{p}_s$ 是两两不同的素理想，α_i，$\beta_i\geqslant 0$（这里我们允许 α_i 或 β_i 为 0，是为了 $\mathfrak{a}$ 和 $\mathfrak{b}$ 的分解式在形式上出现同样的 $\mathfrak{p}_1,\cdots,\mathfrak{p}_s$）. 则

(1) $\mathfrak{a}|\mathfrak{b}\Longleftrightarrow\alpha_i\leqslant\beta_i(1\leqslant i\leqslant s)\Longleftrightarrow\mathfrak{b}\subseteq\mathfrak{a}$.

(2) $\mathfrak{a}+\mathfrak{b}=\prod_{i=1}^{s}\mathfrak{p}_i^{\min(\alpha_i,\beta_i)}$，　$\mathfrak{a}\cap\mathfrak{b}=\prod_{i=1}^{s}\mathfrak{p}_i^{\max(\alpha_i,\beta_i)}$.

(3) 每个分式理想 M 均可唯一表成两个互素的整理想之商，即 $M=\mathfrak{a}\mathfrak{b}^{-1}$，$\mathfrak{a}$ 和 $\mathfrak{b}$ 为整理想并且 $\mathfrak{a}+\mathfrak{b}=R$.

(4) 每个分式理想均可唯一地写成

$$M=\mathfrak{p}_1^{\alpha_1}\cdots\mathfrak{p}_s^{\alpha_s}$$

其中 $\mathfrak{p}_1,\cdots,\mathfrak{p}_s$ 为两两不同的素理想，$\alpha_1,\cdots,\alpha_s$ 为非零整数.

(5) $I(R)$（分式理想群）是以 Spec $R-\{0\}$为基的自由交换群.

证明 (1) 设 $\mathfrak{a}|\mathfrak{b}$，由定义可知有整理想 $\mathfrak{c}$ 使得 $\mathfrak{a}\mathfrak{c}=\mathfrak{b}$. 设 $\mathfrak{c}=\mathfrak{q}_1^{r_1}\cdots\mathfrak{q}_t^{r_t}$ 为 $\mathfrak{c}$ 的素理想分解式. 则 $\mathfrak{p}_1^{\alpha_1}\cdots\mathfrak{p}_s^{\alpha_s}\mathfrak{q}_1^{r_1}\cdots\mathfrak{q}_t^{r_t}=\mathfrak{p}_1^{\beta_1}\cdots\mathfrak{p}_s^{\beta_s}$. 从而由素理想分解式的唯一性可知 $\{\mathfrak{q}_1,\cdots,\mathfrak{q}_t\}\subseteq\{\mathfrak{p}_1\cdots,\mathfrak{p}_s\}$. 令 $\mathfrak{c}=\mathfrak{p}_1^{\delta_1}\cdots\mathfrak{p}_s^{\delta_s}$ $(\delta_i\geqslant 0)$. 则 $\alpha_i\leqslant\alpha_i+\delta_i=\beta_i$ $(1\leqslant i\leqslant s)$，从而 $\mathfrak{b}\subseteq\mathfrak{a}$. 反之若 $\mathfrak{b}\subseteq\mathfrak{a}$，则 $\mathfrak{b}\mathfrak{a}^{-1}\subseteq\mathfrak{a}\mathfrak{a}^{-1}=R$，因此 $\mathfrak{b}\mathfrak{a}^{-1}=\mathfrak{c}$为 R 的整理想. 由于 $\mathfrak{a}\mathfrak{c}=\mathfrak{a}\mathfrak{a}^{-1}\mathfrak{b}=\mathfrak{b}$. 从而 $\mathfrak{a}|\mathfrak{b}$.

(2) $\mathfrak{a}+\mathfrak{b}$ 是可以整除 $\mathfrak{a}$ 和 $\mathfrak{b}$ 的最小理想. $\mathfrak{a}\cap\mathfrak{b}$ 是可以被 $\mathfrak{a}$ 和 $\mathfrak{b}$ 整除的最大理想. 利用(1)即知 $\prod_{i=1}^{s}\mathfrak{p}_i^{\min(\alpha_i,\beta_i)}$ 和 $\prod_{i=1}^{s}\mathfrak{p}_i^{\max(\alpha_i,\beta_i)}$ 分别满足这两个性质.

(3) 设 M 为 R 的分式理想，则有 $0\neq a\in R$，使 $(a)M=\mathfrak{a}'$ 为 R 的整理想. 令 $(a)+\mathfrak{a}'=\mathfrak{c}$，$(a)=\mathfrak{c}\mathfrak{b}$，$\mathfrak{a}'=\mathfrak{c}\mathfrak{a}$. 则由(2)可知 $\mathfrak{a}$ 和 $\mathfrak{b}$ 是互素的整理想，并且 $\mathfrak{c}\mathfrak{b}M=\mathfrak{c}\mathfrak{a}$. 从而 $M=\mathfrak{a}\mathfrak{b}^{-1}$. 如果又有 $M=\mathfrak{a}'\mathfrak{b}'^{-1}$，其中 $\mathfrak{a}'$ 和 $\mathfrak{b}'$ 是互素的整理想. 令 $\mathfrak{a}=\prod_{i=1}^{n}\mathfrak{p}_i^{\alpha_i}$，$\mathfrak{a}'=$

$\prod_{i=1}^{n} \mathfrak{p}_i^{\alpha'_i}$, $\mathfrak{b}=\prod_{i=1}^{n} \mathfrak{p}_i^{\beta_i}$, $\mathfrak{b}'=\prod_{i=1}^{n} \mathfrak{p}_i^{\beta_i'}$ $(\alpha_i,\ \alpha_i', \beta_i,\ \beta'_i \geqslant 0)$. 则 $\alpha_i+\beta'_i=\alpha'_i+\beta_i, \min(\alpha_i,\beta_i)=\min(\alpha'_i,\ \beta'_i)=0$. 由这些条件可知 $\alpha_i=\alpha_i', \beta_i=\beta_i'(1\leqslant i\leqslant n)$. 即 $\mathfrak{a}=\mathfrak{a}', \mathfrak{b}=\mathfrak{b}'$.

(4) 将(3)中的整理想 $\mathfrak{a}$ 和 $\mathfrak{b}$ 展成素理想乘积即得(4)中展开式，它的唯一性是由于 $\mathfrak{a}$ 和 $\mathfrak{b}$ 的唯一性；(4) 中正指数 α_i 对应的素理想之积为 $\mathfrak{a}$，负指数对应的素理想之积为 $\mathfrak{b}$.

(5) 由(4)直接得出. ▌

最后我们对于 Dedekind 整环再给一个模论的刻画.

定理 6 设 R 为整环，则下列三条件彼此等价：

(1) R 为 Dedekind 整环；

(2) R 的每个整理想均为投射 R-模；

(3) R 的每个分式理想均为投射 R-模.

证明 (2)$\Longleftrightarrow$(3)是显然的，因为对每个分式理想 M，有 $0\neq a\in R$ 使得 aM 为整理想. 而 aM 和 M 作为 R-模是同构的.

(1)$\Longleftrightarrow$(3)：根据定理 5，我们只需证明：分式理想 M 可逆 $\Longleftrightarrow M$ 为投射 R-模.

设 M 可逆，则 $MM^{-1}=R$. 由于 M 是有限生成 R-模，令 $M=Rb_1+\cdots+Rb_n$, $b_i\in K$(K 为 R 的商域). 则有 $a_i\in M^{-1}$ $(1\leqslant i\leqslant n)$，使得 $1=\sum_{i=1}^{n} a_ib_i$. 设 $F=Re_1\oplus\cdots\oplus Re_n$ 为自由 R-模，则有唯一的 R-模满同态 $f:F\to M$，使得 $f(e_i)=b_i(1\leqslant i\leqslant n)$. 于是有 R-模短正合序列 $0\to \mathrm{Ker}f\to F\to M\to 0$. 定义 $g:M\to F$, $g(c)=ca_1e_1+\cdots+ca_ne_n(c\in M)$. 这是 R-模同态，并且对每个 $c\in M$ 均有 $fg(c)=f(ca_1e_1+\cdots+ca_ne_n)=c(a_1b_1+\cdots+a_nb_n)=c$. 从而 $fg=1_M$. 这表明上述短正合序列是分裂的. 于是

$F\cong M\oplus\mathrm{Ker}\,f$. 由于 M 为自由R-模 F 的直和成分，从而 M 为投射 R-模.

反之，设分式理想 M 为投射 R-模. 取 $X=\{b_j\mid j\in J\}$为 R-模 M 的任意一组生成元(例如取 $X=M$ 本身). 固定一个元素 $b_0\in X$. 令 $F=\bigoplus\limits_{j\in J}Re_j$，$f:F\to M$ 为 R-模满同态，使得 $f(e_j)=b_j(j\in J)$.则有R-模短正合序列$0\to\mathrm{Ker}\,f\to F\xrightarrow{f}M\to 0$. 由于 M 是投射 R-模，从而此短正合序列是分裂的. 因此有 R-模同态 $g:M\to F$，使得 $fg=1_M$. 对于每个 $j\in J$，令 $p_j:F\to R$为F 到第 j 坐标分量的投影，即$p_j(\sum\limits_{i\in J}r_ie_i)=r_j$. 又令 $\theta_j=p_jg:M\to R$，$c_j=\theta_j(b_0)$. 则对每个 $c\in M$ 均有

$$cc_j=c\theta_j(b_0)=\theta_j(b_0c)=b_0\theta_j(c).$$

(由 θ_j 为 R-模同态易知对每个 $\alpha\in K$，$x\in M$ 均有 $\theta_j(\alpha x)=\alpha\theta_j(x)$.)从而

$$\begin{aligned}c(c_j/b_0)&=cc_j/b_0=b_0\theta_j(c)/b_0\\&=\theta_j(c)\in R\quad(j\in J).\end{aligned}$$

因此 $c_j/b_0\in(R:M)$. 于是对每个 $c\in M$，

$$g(c)=\sum_{j\in J_1}\theta_j(c)e_j=\sum_{j\in J_1}c(c_j/b_0)e_j$$

其中 $J_1=\{j\in J\mid\theta_j(c)\neq 0\}$是有限集合. 从而

$$c=fg(c)=c\sum_{j\in J_1}(c_j/b_0)b_j,\qquad 1=\sum_{j\in J_1}(c_j/b_0)b_j.$$

由于 $c_j/b_0\in(R:M)$，从而 $R\subseteq M(R:M)$，而 $R\supseteq M(R:M)$是显然成立的. 于是 $M(R:M)=R$. 这就表明 M 是可逆的. ▌

系　每个主理想整环均是 Dedekind 整环.

证明　主理想整环 R 的每个整理想均是无扭 R-模，从而为自由模(见 §2.5)，因此是投射模. 于是由定理 6 知它是 Dedekind 整环. ▌ (该系也可由 Dedekind 整环定义直接证明.)

为了得到更多的 Dedekind 整环，下一个定理是重要的.

定理 7 设 R 是 Dedekind 整环，F 为 R 的商域. E/F 为域的有限扩张(即域 E 是域 F 上有限维向量空间). D 为 R 在 E 中的整闭包，则 D 是 Dedekind 整环.

证明 这个定理的证明需要域论的某些知识.

(1) 先设 E/F 是 n 次可分扩张. 令 Ω 为 E 的代数闭包(将对 E 代数的全部元素添加到 E 上而成的域). 所谓 E 是 F 的可分扩张，是指存在着 n 个不同的嵌入(即域的单同态)$\sigma_i: E\to \Omega(1\leqslant i\leqslant n)$，使得对每个 $a\in F$ 均有 $\sigma_i(a)=a(1\leqslant i\leqslant n)$. 每个有限可分扩张 E/F 均是单扩张，即存在 $\alpha\in E$，使得 $E=F(\alpha)$. 因为存在 $r\in R$ 使得 $r\alpha\in D$. 并且 $F(\alpha)=F(r\alpha)$，所以一开始我们不妨假定 $\alpha\in D$. 这时 $\sigma_i(\alpha)\in\Omega(1\leqslant i\leqslant n)$是 n 个不同的元素(因为$\sigma_i(1\leqslant i\leqslant n)$两两不同). 如果 $f(x)\in F[x]$是 α 在域 F 上的极小多项式，则$f(x)=x^n+a_1x^{n-1}+\cdots+a_n=\prod_{i=1}^{n}(x-\sigma_i(\alpha))$. 即$\sigma_i(\alpha)$均是 $f(x)$的根，从而 $\sigma_i(\alpha)$ 均在 F 上整. 而 $a_1,\cdots,a_n$ 为$\sigma_i(\alpha)(1\leqslant i\leqslant n)$的初等对称函数，从而也在 F上整. 但是 $a_i\in F$并且 R 整闭，从而 $a_i\in R(1\leqslant i\leqslant n)$，即$f(x)\in R[x]$.

我们还知道，$1,\alpha,\alpha^2,\cdots,\alpha^{n-1}$ 是 F-向量空间 E 的一组基. 从而 E 中元素唯一地表成 $\gamma=c_0+c_1\alpha+\cdots+c_{n-1}\alpha^{n-1}$, $c_i\in F$. 于是 $\sigma_i(\gamma)=c_0+c_1\sigma_i(\alpha)+\cdots+c_{n-1}\sigma_i(\alpha)^{n-1}$. 从而

$$N(\gamma)=\prod_{i=1}^{n}\sigma_i(\gamma),\qquad T(\gamma)=\sum_{i=1}^{n}\sigma_i(\gamma)$$

均是$\sigma_1(\alpha),\cdots,\sigma_n(\alpha)$的对称多项式(系数属于$F$)，因此是$a_1,\cdots,a_n$ 的多项式(系数属于 F). 于是 $N(\gamma),T(\gamma)\in F$. 我们称 $N(\gamma)$和 $T(\gamma)$分别是 E 中元素 γ 的范和迹. 不难看出：

(A) $\gamma_1,\gamma_2\in E$，则 $N(\gamma_1\gamma_2)=N(\gamma_1)N(\gamma_2)$，$T(\gamma_1+\gamma_2)=T(\gamma_1)+T(\gamma_2)$.

(B) 若$\gamma\in D$,则 $N(\gamma),T(\gamma)\in R$.(这是因为:若 $\gamma\in D$,即 γ 在 R 上整,则 $\sigma_i(\gamma)$均在 R 上整,从而 $N(\gamma),T(\gamma)$ 也在 R 上整. 但是 $N(\gamma),T(\gamma)\in F$,而 R 整闭,从而 $N(\gamma),T(\gamma)\in R$.)

有了以上这些准备,现在来证明 D 为 Dedekind 环. 首先,对 E 中元素 $x=c_0+c_1\alpha+\cdots+c_{n-1}\alpha^{n-1}(c_i\in F)$. 我们有

$$T(x\alpha^j)=\sum_{i=0}^{n-1}c_iT(\alpha^{i+j})\quad(0\leqslant j\leqslant n-1),\tag{*}$$

注意$T(\alpha^{i+j})\in R$. 考虑方阵

$$(T(\alpha^{i+j}))_{0\leqslant i,j\leqslant n-1}=\begin{pmatrix}1\cdots\cdots\cdots\cdots\cdots 1\\ \sigma_1(\alpha)\ \cdots\cdots\ \sigma_n(\alpha)\\ \cdots\cdots\cdots\cdots\cdots\cdots\\ \sigma_1(\alpha)^{n-1}\cdots\ \sigma_n(\alpha)^{n-1}\end{pmatrix}\begin{pmatrix}1\ \ \sigma_1(\alpha)\cdots\sigma_1(\alpha)^{n-1}\\ \cdots\cdots\cdots\cdots\cdots\cdots\\ 1\ \ \sigma_n(\alpha)\cdots\sigma_n(\alpha)^{n-1}\end{pmatrix}.$$

由于$\sigma_i(\alpha)$两两不同,右边方阵的行列式为 Vandemond 行列式,从而不为 0. 于是令左边阵的行列式为 d,则 $0\neq d\in R$. 而将(*)看成是以 $c_i(0\leqslant i\leqslant n-1)$为变量的线性方程组,即解出为

$$c_i=d^{-1}\sum_{j=1}^{n-1}d_{ij}T(x\alpha^j),\qquad d_{ij}\in R\ (0\leqslant i\leqslant n-1).$$

如果 $x\in D$, 则 $x\alpha^j\in D$, 从而 $T(x\alpha^j)\in R$, 从而 $D\subseteq d^{-1}R$, 由于 R 为 Noether 环,D为有限生成R-模$d^{-1}R$的R-子模,从而 D也为有限生成 R-模.于是D为 Noether 环.

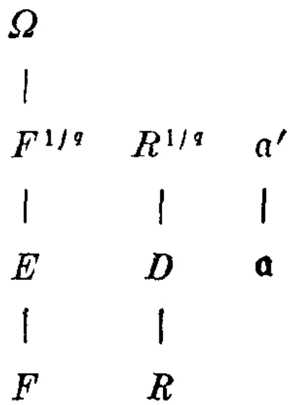
其次,设 $\mathfrak{q}$ 为D中非零素理想. 取 $0\neq r\in\mathfrak{q}$, 则 $f(x)=(x-\sigma_1(r))\cdots(x-\sigma_n(r))\in R[x]$. 从而 $\sigma_2(r)\cdots\sigma_n(r)=\dfrac{N(r)}{\sigma_1(r)}=\dfrac{N(r)}{r}\in F$ (这里我们令 σ_1 为恒等嵌入). 又因 $\sigma_2(r),\cdots,\sigma_n(r)$均在$R$上整,于是 $\sigma_2(r)\cdots\sigma_n(r)\in D$. 从而 $N(r)\in rD\subseteq\mathfrak{q}$. 令 $\mathfrak{p}=\mathfrak{q}\cap R$, 则 $\mathfrak{p}$ 是R的非零素理想(因为 $0\neq N(r)\in\mathfrak{q}\cap R=$

$\mathfrak{p}$). 由于R为 Dedekind 环，从而 $\mathfrak{p}$ 为R的极大理想．因为 $R\subseteq D$ 是环的整性扩张，从而 $\mathfrak{q}$ 也为D的极大理想．于是 $\dim D=1$.

最后，E 中元素均可写成 a/r, $a\in D$, $r\in R\subseteq D$. 因此E是 D 的商域，而D为R在E中的整闭包，从而D是整闭整环．综合上述，即知D是 Dedekind 整环．

(2) 设 E/F 为纯不可分的有限扩张，并且 $E\neq F$，这时F的特征为素数 p. 并且有 $q=p^l(l\geqslant 1)$，使得 $E^q\subseteq F$. 仍以 Ω 表示 E 的代数闭包．则 $F^{1/q}=\{v\in\Omega\mid v^q\in F\}$ 是 E 的扩域．$R^{1/q}=\{v\in\Omega\mid v^q\in R\}$为 $F^{1/q}$ 的子环，并且 $D\subseteq R^{1/q}$. 易知 $f: F^{1/q}\to F$, $v\mapsto v^q$ 为域的同构，并且 f 在 $R^{1/q}$ 上的限制给出环的同构 $R^{1/q}\cong R$. 于是 $R^{1/q}$ 也是 Dedekind 整环．

现在为证D是 Dedekind 整环，只需证 D 的每个整理想 $\mathfrak{a}$ 均可逆．将 $\mathfrak{a}$ 扩充成 $R^{1/q}$ 中的理想 $\mathfrak{a}'=R^{1/q}\mathfrak{a}$ (如图所示).



由于$R^{1/q}$为 Dedekind 整环，从而有 $R^{1/q}$ 的分式理想 $\mathfrak{b}'$，使得 $\mathfrak{a}'\mathfrak{b}'=R^{1/q}$. 由于 $\mathfrak{a}'=\mathfrak{a}R^{1/q}$, $\mathfrak{b}'R^{1/q}=\mathfrak{b}'$，从而有 $a_i\in\mathfrak{a}$, $b_i'\in\mathfrak{b}'$,

使得$1=\sum\limits_{i=1}^{n} a_ib_i'$,

从而 $1=\sum\limits_{i=1}^{n} a_i^qb_i'^q=\sum\limits_{i=1}^{n} a_ic_i$，其中 $c_i=a_i^{q-1}b_i'^q\in\mathfrak{a}_i'^{q-1}\mathfrak{b}'^q\subseteq\mathfrak{b}'$.

另一方面，$b_i'^q\in F$, $a_i\in E$. 于是 $c_i\in E\cap\mathfrak{b}'=\mathfrak{b}$, $\mathfrak{b}$ 是D的分式理想．

从而由 $1=\sum_{i=1}^{n}a_ic_i, a_i\in\mathfrak{a}$，$c_i\in\mathfrak{b}$ 可知 $\mathfrak{ab}\supseteq D$．但是 $\mathfrak{ab}\subseteq R^{1/q}\cap E=D$．于是 $\mathfrak{ab}=D$．这就表明 $\mathfrak{a}$ 为可逆理想．即 D 为 Dedekind 整环．

(3) 最后，对于任意的有限扩张 E/F，熟知存在中间域 M，$F\subseteq M\subseteq E$，使得 M/F 为可分扩张而 E/M 为纯不可分扩张．令 S 为 R 在 M 中的整闭包，则 S 在 E 中的整闭包即是 R 在 E 中的整闭包 D．由(1)知 S 为 Dedekind 整环，再由(2) 即知 D 为 Dedekind 整环．这就完全证明了定理 7．▌

注记 这个定理对于代数数论和代数几何(代数函数论)是很基本的．这是因为：

(I) 我们知道，**Z** 是 Dedekind 整环(定理 6 的系)．设 K 是 **Q** 的有限次扩域．O_K 是 **Z** 在 K 中的整闭包，则由定理 7 可知 O_K 是 Dedekind 整环．通常称 K 为代数数域而 O_K 为域 K 的整数环，这是代数数论的一个主要研究对象(详见第六章)．

(II) 设 k 为域，则 $k[x]$ 为主理想整环，从而为 Dedekind 整环．它的商域为有理函数域 $k(x)$．设 $K/k(x)$ 为有限次代数扩张，O_K 为 $k[x]$ 在 K 中的整闭包，由定理 7 知道 O_K 为 Dedekind 整环．通常称这里的 K 为单变量的代数函数域，它是代数几何中某个代数曲线的有理函数域(详见第六章)，而对 Dedekind 整环 O_K 的分析则与研究代数曲线的覆盖和分歧性有直接联系．

现在我们谈第二个题目：Dedekind 整环上有限生成模的结构和分类问题．我们在 § 2.6 中给出主理想整环上这个问题的完整结果，在 Dedekind 整环上我们也有非常类似的完整结论．

引理 12 设 R 是 Dedekind 整环，M 为有限生成无扭 R-模．则

(1) M 同构于某个 R^t 的 R-子模．

(2) M作为R-模同构于R中有限个整理想的直和.

(3) M是投射R-模.

证明 (1)设$M=Ru_1+\cdots+Ru_r$,不妨设$M\neq(0)$,$\{u_1,\cdots,u_s\}$为$\{u_1,\cdots,u_r\}$的一个极大R-线性无关子集合,则自由R-模$N=Ru_1\oplus\cdots\oplus Ru_s$为$M$的子模. 另一方面,对于每个$j\geqslant1$,$\{u_{s+j},u_1,\cdots,u_s\}$均是$R$-线性相关的. 从而有不全为0的$d_i\in R$使得$d_1u_1+\cdots+d_su_s+d_{s+j}u_{s+j}=0$. 由于$u_1,\cdots,u_s$线性无关可知$d_{s+j}\neq0$,并且$d_{s+j}u_{s+j}=-(d_1u_1+\cdots+d_su_s)\in N$. 令$d=d_{s+1}\cdots d_r\neq0$,则$dM\subseteq N$. 但是我们有$R$-模同构$M\simeq dM$,$x\mapsto dx$,而$dM\subseteq N$,从而$M$同构于自由模$N$的子模,$N\cong R^s$.

(2) 由(1)知M为某个自由R-模$Ru_1\oplus\cdots\oplus Ru_s$的子模. 当$s=1$时,$M$同构于$R$的$R$-子模,即$M$同构于$R$的某个理想. 现设命题对$\leqslant s-1$均成立,令$S=Ru_1\oplus\cdots\oplus Ru_{s-1}$,这是$Ru_1\oplus\cdots\oplus Ru_s$的子模.考虑$R$-模同态$p:M\to R$,$p(r_1e_1+\cdots+r_se_s)=r_s$. 则$\mathfrak{a}=p(M)$为$R$的理想. $N=\mathrm{Ker}\,p$为S的子模. 并且有R-模短正合序列$0\to N\to M\xrightarrow{p}\mathfrak{a}\to0$.由于$\mathfrak{a}$是投射$R$-模,从而$M\cong N\oplus\mathfrak{a}$. 而由归纳假设,$S(\cong R^{s-1})$的子模$N$同构于有限个理想的直和,从而$M\cong N\oplus\mathfrak{a}$也是如此.

(3) 根据(2),我们有R-模同构$M\cong\mathfrak{a}_1\oplus\cdots\oplus\mathfrak{a}_n$,$\mathfrak{a}_i$均为$R$的理想,从而$\mathfrak{a}_i$均是投射$R$-模. 于是$M$也是投射$R$-模. ▮

由此可证明与主理想整环情形完全一样的一个结果:

定理 8 设R是Dedekind整环,M为有限生成R-模,$T(M)$为M的扭子模,则存在M的无扭子模M'使得$M=T(M)\oplus M'$.

证明 我们有R-模短正合序列$0\to T(M)\to M\to M/T(M)\to0$. 而$M/T(M)$是无扭的,从而由引理12知$M/T(M)$为投射$R$-模. 于是这个短正合序列是分裂的. 从而$T(M)$是$M$的直和成分. 即存在$M$的子模$M'$使得$M=T(M)\oplus M'$. 而$M'\cong M/T(M)$,从而$M'$是$M$的无扭子模. ▮

注记 M'不是唯一决定的. 但是若又有 $M=T(M)\oplus M''$ 则M'和M''同构.

定理 8 将问题化为扭模和无扭模两种情形. 先谈无扭模的情形. 在主理想整环上的有限生成无扭模均是自由模. 而在引理12中我们证明了, Dedekind 整环上的有限生成无扭模是R中有限个理想的直和. 但这还不是最后结果, 为了给出进一步的结构和分类, 我们需要下面引理.

引理 13 设 $\mathfrak{a}_1,\mathfrak{a}_2$ 是Dedekind整环R的两个非零理想, 则有R-模同构$\mathfrak{a}_1\oplus\mathfrak{a}_2\cong R\oplus\mathfrak{a}_1\mathfrak{a}_2$.

证明 引理 13 的证明依赖于一个技术性的结果: 我们证明存在$a_1\in\mathfrak{a}_1, a_2\in\mathfrak{a}_2, b_1\in\mathfrak{a}_1^{-1}, b_2\in\mathfrak{a}_2^{-1}$, 使得$a_1b_1+a_2b_2=1$. 方法是: 任取$0\neq a_2\in\mathfrak{a}_2$, 则$a_2\mathfrak{a}_2^{-1}\subseteq\mathfrak{a}_2\mathfrak{a}_2^{-1}=R$, 从而$a_2\mathfrak{a}_2^{-1}$为$R$的整理想. 如果 $a_2\mathfrak{a}_2^{-1}=R$, 则有 $b_2\in\mathfrak{a}_2^{-1}$ 使得 $a_2b_2=1$. 于是取 $a_1=b_1=0$ 即有 $a_1b_1+a_2b_2=1$. 如果$a_2\mathfrak{a}_2^{-1}\neq R$, 则$a_2\mathfrak{a}_2^{-1}$是$R$的非零真理想. 从而 $a_2\mathfrak{a}_2^{-1}=\mathfrak{p}_1^{\alpha_1}\cdots\mathfrak{p}_t^{\alpha_t}$, 其中$\mathfrak{p}_1,\cdots,\mathfrak{p}_t$为$R$的两两不同的素理想, $\alpha_i\geqslant 1$. 取$c_i\in\mathfrak{a}_1\mathfrak{p}_1\cdots\mathfrak{p}_{i-1}\mathfrak{p}_{i+1}\cdots\mathfrak{p}_t-\mathfrak{a}_1\mathfrak{p}_1\cdots\mathfrak{p}_t$ $(1\leqslant i\leqslant t)$, 则 $c_i\mathfrak{a}_1^{-1}$ 均为R的整理想, 并且

$$c_i\mathfrak{a}_1^{-1}\subseteq\mathfrak{p}_j\,(\text{当 } i\neq j \text{ 时}),\quad c_i\mathfrak{a}_1^{-1}\nsubseteq\mathfrak{p}_i\ (1\leqslant i\leqslant t).$$

令$a_1=c_1+\cdots+c_t$, 则由以上两式可知$a_1\mathfrak{a}_1^{-1}\nsubseteq\mathfrak{p}_i(1\leqslant i\leqslant t)$. 由于$c_i\in\mathfrak{a}_1(1\leqslant i\leqslant t)$, 从而$a_1\in\mathfrak{a}_1$, 即$a_1\mathfrak{a}_1^{-1}$是整理想. 注意$a_2\mathfrak{a}_2^{-1}$的素理想因子$\mathfrak{p}_i(1\leqslant i\leqslant t)$均不是$a_1\mathfrak{a}_1^{-1}$的因子. 从而$a_2\mathfrak{a}_2^{-1}$和$a_1\mathfrak{a}_1^{-1}$是互素的整理想. 因此$a_1\mathfrak{a}_1^{-1}+a_2\mathfrak{a}_2^{-1}=R$. 这就表明存在$b_1\in\mathfrak{a}_1^{-1}$和$b_2\in\mathfrak{a}_2^{-1}$使得$a_1b_1+a_2b_2=1$.

现在作映射:

$$f:\mathfrak{a}_1\oplus\mathfrak{a}_2\to R\oplus\mathfrak{a}_1\mathfrak{a}_2,\qquad f(x_1,x_2)=(x_1,x_2)\begin{pmatrix}b_1 & -a_2\\ b_2 & a_1\end{pmatrix}$$
$$=(b_1x_1+b_2x_2,\ a_1x_2-a_2x_1),$$

$$g: R\oplus\mathfrak{a}_1\mathfrak{a}_2\to\mathfrak{a}_1\oplus\mathfrak{a}_2,\quad g\ (y_1,y_2)=(y_1,y_2)\begin{pmatrix} a_1 & a_2\\ -b_2 & b_1\end{pmatrix}$$
$$=(a_1y_1-b_2y_2, a_2y_1+b_1y_2).$$

f 和 g 均是 R-模同态，并且可直接验证它们互逆．从而有 R-模同构 $\mathfrak{a}_1\oplus\mathfrak{a}_2\cong R\oplus\mathfrak{a}_1\mathfrak{a}_2$．▌

定理 9 （无扭模情形） 设 R 为Dedekind整环，K 为 R 的商域．$\mathfrak{a}_i,\mathfrak{b}_j$ 是 R 的非零理想，则下列两条件等价：

(1) $\mathfrak{a}_1\oplus\cdots\oplus\mathfrak{a}_n\cong\mathfrak{b}_1\oplus\cdots\oplus\mathfrak{b}_m$ （R-模同构）；

(2) $n=m$ 并且存在 $0\neq\alpha\in K$，使得 $\mathfrak{a}_1\cdots\mathfrak{a}_n=(\alpha)\mathfrak{b}_1\cdots\mathfrak{b}_n$．

证明 根据引理 13 我们有 R-模同构 $\mathfrak{a}_1\oplus\cdots\oplus\mathfrak{a}_n=R^{n-1}\oplus\mathfrak{a}$, $\mathfrak{b}_1\oplus\cdots\oplus\mathfrak{b}_m=R^{m-1}\oplus\mathfrak{b}$，其中 $\mathfrak{a}=\mathfrak{a}_1\cdots\mathfrak{a}_n$, $\mathfrak{b}=\mathfrak{b}_1\cdots\mathfrak{b}_m$．

(2) $\Rightarrow$(1)：如果 $n=m$，并且 $\mathfrak{a}=(\alpha)\mathfrak{b}$，则有 R-模同构 $\mathfrak{a}=(\alpha)\mathfrak{b}\cong\mathfrak{b}$．于是 $R^{n-1}\oplus\mathfrak{a}\cong R^{m-1}\oplus\mathfrak{b}$．

(1)$\Rightarrow$(2)：假设 $R^{n-1}\oplus\mathfrak{a}\cong R^{m-1}\oplus\mathfrak{b}$．令 $S=R-\{0\}$．对于 R 的每个非零理想 $\mathfrak{c}$，$\mathfrak{c}\cap S\neq\varnothing$．从而 $S^{-1}\mathfrak{c}=K$．于是 $S^{-1}(R^{n-1}\oplus\mathfrak{a})\cong K^n$, $S^{-1}(R^{m-1}\oplus\mathfrak{b})\cong K^m$．这就得出 $n=m$．于是有 R-模同构 $R^{n-1}\oplus\mathfrak{a}\cong R^{n-1}\oplus\mathfrak{b}$．设其互逆的 R-模同构为 $f: R^{n-1}\oplus\mathfrak{a}\simeq R^{n-1}\oplus\mathfrak{b}$ 和 $g: R^{n-1}\oplus\mathfrak{b}\simeq R^{n-1}\oplus\mathfrak{a}$．转到对乘法集 $S=R-\{0\}$ 的分式模上之后，便有 K-向量空间同构 $\tilde{f}: K^{n-1}\oplus K\simeq K^{n-1}\oplus K$ 和 $\tilde{g}: K^{n-1}\oplus K\simeq K^{n-1}\oplus K$．其中 f 和 g 分别是 $\tilde{f}$ 和 $\tilde{g}$ 的限制映射，并且 $\tilde{f}$ 和 $\tilde{g}$ 互逆．令 F 和 G 分别是 $\tilde{f}$ 和 $\tilde{g}$ 的变换方阵．则对每个 $a\in\mathfrak{a}$，我们有

$$\begin{pmatrix} 1 & 0 & \cdots & 0 & a\\ 0 & 1 & \cdots & 0 & a\\ \cdots & \cdots & \cdots & \cdots & \cdots\\ 0 & 0 & \cdots & 1 & a\\ 0 & 0 & \cdots & 0 & a\end{pmatrix}F=\begin{pmatrix} y_{11} & \cdots & y_{1,n-1} & b_1\\ \cdots & \cdots & \cdots & \cdots\\ y_{n,1} & \cdots & y_{n,n-1} & b_n\end{pmatrix},$$

其中 $b_i\in\mathfrak{b}(1\leqslant i\leqslant n)$, $y_{ij}\in R$. 两边取行列式可知 $a\cdot(\det F)\in\mathfrak{b}$, 于是 $(\det F)\cdot\mathfrak{a}\subseteq\mathfrak{b}$. 同样地有 $(\det G)\mathfrak{b}\subseteq\mathfrak{a}$. 但是 $\det F\cdot\det G=\det(F\ G)=\det(I_n)=1$. 从而 $\mathfrak{a}\subseteq(\det G)\mathfrak{b}$, 即 $\mathfrak{a}=(\det G)\mathfrak{b}$. 取 $\alpha=\det G$, 则 $0\neq\alpha\in K$, 而 $\mathfrak{a}=(\alpha)\mathfrak{b}$. ▮

现在谈扭模情形. 首先需要一个有趣的引理.

引理 14 只有有限个素理想的 Dedekind 整环 R 必为主理想整环.

证明 设 $\mathfrak{p}_1,\cdots,\mathfrak{p}_n$ 为 R 的全部非零素理想. 对 R 的每个整理想 $\mathfrak{a}$, 不妨设 $\mathfrak{a}\neq(0),(1)$. 则 $\mathfrak{a}=\mathfrak{p}_1^{\alpha_1}\cdots\mathfrak{p}_n^{\alpha_n}$ $(\alpha_i\geqslant 0)$. 取 $a_i\in\mathfrak{a}\mathfrak{p}_1\cdots\mathfrak{p}_{i-1}\mathfrak{p}_{i+1}\cdots\mathfrak{p}_n-\mathfrak{a}\mathfrak{p}_1\cdots\mathfrak{p}_n(1\leqslant i\leqslant n)$, $a=a_1+\cdots+a_n$, 可象引理 13 的证明中一样证得 $a\mathfrak{a}^{-1}=R$. 于是 $\mathfrak{a}=(a)$. 即 R 为主理想整环. ▮

定理 10 (扭模情形)设 R 为 Dedekind 整环, M 是有限生成的扭 R-模, $M\neq(0)$. 则

(1) 存在 R 的 m 个理想 $\mathfrak{a}_i$, $R\neq\mathfrak{a}_1\supseteq\mathfrak{a}_2\supseteq\cdots\supseteq\mathfrak{a}_m\neq(0)$. 使得 $M\cong R/\mathfrak{a}_1\oplus\cdots\oplus R/\mathfrak{a}_m$ (R-模同构).

(2) m 和 $\mathfrak{a}_1,\cdots,\mathfrak{a}_m$ 是由 M 所唯一决定的.

证明 (1)设 $M=Ru_1+\cdots+Ru_n(n\geqslant 1)$. 由于 u_i 均为扭元素, 从而 $\mathrm{Ann}(u_i)\neq(0)$. 于是 $\mathrm{Ann}(M)=\bigcap_{i=1}^{n}\mathrm{Ann}(u_i)\neq(0)$. 又因为 $M\neq(0)$, 从而 $\mathrm{Ann}(M)$ 为 R 的真理想. 令 $\{\mathfrak{p}_1,\cdots,\mathfrak{p}_r\}$ 为 $\mathrm{Ann}(M)$ 的全部素理想因子, 则 $r\geqslant 1$. 令 $S=R-\bigcup_{i=1}^{r}\mathfrak{p}_i=\bigcap_{i=1}^{r}(R-\mathfrak{p}_i)$, 这是 R 的乘法集. 于是 $\mathfrak{p}_i\cap S=\varnothing(1\leqslant i\leqslant r)$, 而对每个其他的非零素理想 $\mathfrak{p}$, $\mathfrak{p}\cap S\neq\varnothing$. (由于 $\mathfrak{p},\mathfrak{p}_1,\cdots,\mathfrak{p}_r$ 是两两互素的, 由中国剩余定理可知存在 $x\in R$ 使得 $x\equiv 0(\mathrm{mod}\ \mathfrak{p})$, $x\equiv 1(\mathrm{mod}\ \mathfrak{p}_i)(1\leqslant i\leqslant r)$, 于是 $x\in\mathfrak{p}\cap S$.) 因此分式环 $R_S=S^{-1}R$ 中只有有限多非零素

理想 $\mathfrak{p}_i R_S(1\leqslant i\leqslant r)$. 但是 R_S 也是 Dedekind整环，从而由引理14 可知 R_S 是主理想整环，而 $M_S=S^{-1}M=R_S u_1+\cdots+R_S u_r$ 是有限生成的扭 R_S-模. 利用主理想整环上的结果，即知

$$M_S\cong R_S/\mathfrak{b}_1\oplus\cdots\oplus R_S/\mathfrak{b}_m,\quad R_S\supsetneqq\mathfrak{b}_1\supseteq\mathfrak{b}_2\supseteq\cdots\supseteq\mathfrak{b}_m\supsetneqq(0),$$

$\mathrm{Ann}(M_S)=\mathfrak{b}_m$, $\mathfrak{b}_i$ 均为 R_S 的理想. 对于每个元素 $a\in S$, (a)与 $\mathrm{Ann}(M)$互素. 从而 $\bar{a}$ 为$R/\mathrm{Ann}(M)$中的单位. 所以有 R-模同构$(R/\mathrm{Ann}(M))_S\cong R/\mathrm{Ann}(M)$. 于是又有$R$-模同构

$$\begin{aligned}M&\cong M/(\mathrm{Ann}(M))M\cong M\otimes_R(R/\mathrm{Ann}(M))\\&\cong M\otimes_R(R/\mathrm{Ann}(M))_S\cong M\otimes_R(R_S\otimes_R(R/\mathrm{Ann}(M)))\\&\cong(M\otimes_R R_S)\otimes_R(R/\mathrm{Ann}(M))\cong M_S\otimes_R(R/\mathrm{Ann}(M)).\end{aligned}$$

记 $\mathfrak{a}_i=\mathfrak{b}_i\cap R$, 这是 R 的理想，并且 $R\supsetneqq\mathfrak{a}_1\supseteq\mathfrak{a}_2\supseteq\cdots\supseteq\mathfrak{a}_m\supsetneqq(0)$, $(\mathfrak{a}_i)_S=\mathfrak{b}_i$. $\mathrm{Ann}(M)=(\mathrm{Ann}(M_S))^c=\mathfrak{b}_m^c=\mathfrak{a}_m$. 于是又有$R$-模同构

$$\begin{aligned}R/\mathfrak{a}_i&\cong(R/\mathfrak{a}_i)/\mathrm{Ann}(M)\cdot(R/\mathfrak{a}_i)\cong R/\mathfrak{a}_i\otimes_R R/\mathrm{Ann}(M)\\&\cong(R/\mathfrak{a}_i)_S\otimes_R(R/\mathrm{Ann}(M))\cong R_S/\mathfrak{b}_i\otimes_R R/\mathrm{Ann}(M).\end{aligned}$$

从而 $M\cong M_S\otimes_R(R/\mathrm{Ann}(M))\cong\left(\bigoplus\limits_{i=1}^{r}R_S/\mathfrak{b}_i\right)\otimes_R(R/\mathrm{Ann}(M))$

$$\cong\bigoplus_{i=1}^{r}(R_S/\mathfrak{b}_i\otimes_R R/\mathrm{Ann}(M))\cong\bigoplus_{i=1}^{r}R/\mathfrak{a}_i.$$

(2)m 由 M_S 决定，从而由 M 和 $\mathrm{Ann}(M)$决定，于是仅由M决定. 另一方面，$\mathfrak{b}_1,\cdots,\mathfrak{b}_m$ 也是由 M_S 决定的，从而 $\mathfrak{a}_i=\mathfrak{b}_i\cap R$ $(1\leqslant i\leqslant r)$也是由 R-模M所决定的. ▌

定理 9 和定理 10 完整地解决了 Dedekind 整环上有限生成模的结构和分类问题.

最后谈谈 Dedekind 整环的类群问题. 我们已经证明了，主理想整环均是 Dedekind 整环. 下面例子表明反过来不必成立.

例 7 考虑域$K=\mathbf{Q}(\sqrt{-5})$. 设 Ω 是它的代数闭包. 则 σ_i: $\mathbf{Q}(\sqrt{-5})\to\Omega(i=1,2)$是两个不同的嵌入，其中 σ_1为恒等嵌入，

而$\sigma_2(\alpha+\beta\sqrt{-5})=\alpha-\beta\sqrt{-5}(\alpha,\beta\in\mathbf{Q})$. $\mathbf{Q}(\sqrt{-5})/\mathbf{Q}$ 是二次扩张. 根据定理 7 可知 $\mathbf{Z}$ 在 $\mathbf{Q}(\sqrt{-5})$中的整闭包O_K是 Dedekind 整环. 我们现在决定 O_K: K 的元素均可唯一地表成 $\alpha+\beta\sqrt{-5},\alpha,\beta\in\mathbf{Q}$, 它的范和迹分别为 $\alpha^2+5\beta^2$和 2α. 如果$\alpha+\beta\sqrt{-5}\in O_K$, 则 $\alpha^2+5\beta^2$和 2α 均属于 $\mathbf{Z}$. 由数论知识可知 α, $\beta\in\mathbf{Z}$. 反之,若 $\alpha,\beta\in\mathbf{Z}$,则 $\alpha+\beta\sqrt{-5}$ 是首一多项式 $x^2-2\alpha x+\alpha^2+5\beta^2=0$ 的根. 从而$\alpha+\beta\sqrt{-5}\in O_K$. 这就证明$O_K=\{\alpha+\beta\sqrt{-5}|\alpha,\beta\in\mathbf{Z}\}=\mathbf{Z}[\sqrt{-5}]$. 于是 $\mathbf{Z}[\sqrt{-5}]$ 为 Dedekind 整环,但它不是主理想整环. 比如$(2,1+\sqrt{-5})$就不是主理想. 因若$(2,1+\sqrt{-5})=(a+b\sqrt{-5}),a,b\in\mathbf{Z}$,则有 $c,d\in\mathbf{Z}$ 使得 $2=(a+b\sqrt{-5})(c+d\sqrt{-5})$,取范则 $4=(a^2+5b^2)(c^2+5d^2)$. 这只可能 $a=\pm2,b=0$. 从而$(2,1+\sqrt{5})=(2)$. 但这是不可能的, 因为$1+\sqrt{5}\notin(2)$. 总之, $\mathbf{Z}[\sqrt{-5}]$为 Dedekind 整环但不是主理想整环.

这就使我们产生了一个问题:何时一个 Dedekind 整环是主理想整环? 或者更一般地,如果 Dedekind 整环不是主理想整环, 如何来衡量它与主理想整环相差的程度? 这就是所谓"理想类群"的概念.

我们知道,对于每个 Dedekind 整环 R,R 的全部分式理想形成乘法群 $I(R)$. 不难看出,其中主分式理想形成它的一个子群 $P(R)((\alpha)(\beta)=(\alpha\beta),(\alpha)^{-1}=(\alpha^{-1}))$, 叫作是 R 的**主分式理想群**. 它们都是交换群,其商群 $C(R)=I(R)/P(R)$叫作是R的**理想类群**. 每个分式理想 $\mathfrak{a}$ 在 $C(R)$ 中的象,叫作是 $\mathfrak{a}$ 所在的**理想类**. 于是两个分式理想$\mathfrak{a}$和 $\mathfrak{b}$ 属于同一个理想类,当且仅当它们相差一个主分式理想, 即存在 $0\neq\alpha\in K$ (K 为 R 的商域),使得 $\mathfrak{a}=(\alpha)\mathfrak{b}$. 特别地,

$C(R)$为一元群$\Longleftrightarrow I(R)=P(R)\Longleftrightarrow R$的每个分式理想均是主分式理想$\Longleftrightarrow R$的每个整理想均是主理想$\Longleftrightarrow R$为主理想整环.

于是,$C(R)$的大小可以用来衡量 Dedekind 整环R与主理想整环相距程度. 代数数论的一个重要结果是: 如果K是代数数域(即K为$\mathbf{Q}$的有限次扩张),O_K是K的(代数)整数环(即$\mathbf{Z}$在K中的整闭包),则 Dedekind 整环O_K的理想类群$C(O_K)$必是有限交换群. 记$h(K)$为有限群$C(O_K)$的阶数,称作是代数数域K(或者O_K)的**理想类数**. 对于类群$C(O_K)$和类数$h(K)$的研究,是代数数论中心议题之一.

我们说过, Gauss 和 Kummer 等人对于环中元素分解问题感兴趣. 比如,Gauss 研究过环$\mathbf{Z}[\sqrt{-1}]$. 他证明了这个环中也象整数环$\mathbf{Z}$那样,每个元素唯一地分解成有限个"素数"的乘积. 具有这类性质的环就是我们在近世代数中学过的唯一因子分解整环. Kummer 于 1847 年"证明"了著名的 Fermat 猜想,就是他假定了代数数域F的整数环O_F均是唯一因子分解整环. 但这是不对的. 然而 Kummer 引进了"理想"这一重要概念. 我们在第六章还要提到这段往事. 现在的问题是:何时一个 Dedekind 整环是唯一因子分解整环?

如果 Dedekind 整环R的理想类数为 1, 则R为主理想整环, 从而R也是唯一因子分解整环. 因为我们在近世代数中学过, 每个主理想整环必然是唯一因子分解整环. 一般来说, 唯一因子分解整环不必是主理想整环(比如环$k[x,y]$, 其中k为域就是这样的例子). 可是,我们现在要证明:如果R已假定是 Dedekind 整环,那末如果R又是唯一因子分解整环,它就一定是主理想整环. 换句话说,对于 Dedekind 整环R,理想类数为 1 也是R成为唯一因子分解整环的充要条件.

定理 11 如果R为 Dedekind 整环, 并且又是唯一因子分解

整环，则 R 是主理想整环.

证明 设 $\mathfrak{a}$ 为 R 的非零理想，$\mathfrak{a}=Ra_1+\cdots+Ra_n$. 由于 $\mathfrak{a}$ 可逆，从而 $1=\sum_{i=1}^{n}a_ib_i$，$b_i\in\mathfrak{a}^{-1}\subseteq K$（$K$ 为 R 的商域）. 令 $b_i=c_i/d_i$，$c_i,d_i\in R$，$(c_i,d_i)=1$（注意：唯一因子分解整环中存在着元素整除性，最大的因子 (c_i,d_i) 和最小公倍元 $[c_i,d_i]$ 这些概念）. 由于 $(c_i/d_i)\cdot a_j\in\mathfrak{a}^{-1}\mathfrak{a}\subseteq R$ 而 $(c_i,d_i)=1$，因此 $d_i\,|\,a_j(1\leqslant i,j\leqslant n)$. 记 $d=[d_1,\cdots,d_n]$，则 $d\,|\,a_j(1\leqslant j\leqslant n)$. 从而 $a_j\in(d)\ (1\leqslant j\leqslant n)$，即 $\mathfrak{a}\subseteq(d)$. 另一方面，

$$d=d\cdot\sum_{i=1}^{n}a_i(c_i/d_i)=\sum_{i=1}^{n}a_ic_i(d/d_i)\in\mathfrak{a}$$

（因为 $a_i\in\mathfrak{a},c_i,d/d_i\in R$），从而 $(d)\subseteq\mathfrak{a}$. 于是 $\mathfrak{a}=(d)$. 即 R 是主理想整环. ▌

习　　题

（以下 D 为 Dedekind 整环，K 是 D 的商域）

1．设 $\mathfrak{a},\mathfrak{b}$ 为 D 的分式理想. 如果 $\mathfrak{b}\mathfrak{a}^{-1}$ 为整理想，则称 $\mathfrak{a}$ 整除 $\mathfrak{b}$，并表示成 $\mathfrak{a}\,|\,\mathfrak{b}$. 求证

(1) $\mathfrak{a}\,|\,\mathfrak{b}\Longleftrightarrow\mathfrak{a}\supseteq\mathfrak{b}$.

(2) 设 $\mathfrak{a}=\mathfrak{p}_1^{\alpha_1}\cdots\mathfrak{p}_s^{\alpha_s}$，$\mathfrak{b}=\mathfrak{p}_1^{\beta_1}\cdots\mathfrak{p}_s^{\beta_s}$，其中 $\mathfrak{p}_1,\cdots,\mathfrak{p}_s$ 为 D 中不同的非零素理想，$\alpha_i,\beta_i\in\mathbf{Z}$. 则 $\mathfrak{a}\,|\,\mathfrak{b}\Longleftrightarrow\alpha_i\leqslant\beta_i(1\leqslant i\leqslant s)$.

2．设 $\mathfrak{a},\mathfrak{b}$ 为 D 的两个分式理想. 求证 $(\mathfrak{a}+\mathfrak{b})(\mathfrak{a}\cap\mathfrak{b})=\mathfrak{a}\mathfrak{b}$.

3．设 $(0)\neq\mathfrak{p}\in\operatorname{Spec}D$，$\mathfrak{a}$ 为分式理想. 求证

(1) 存在唯一的整数 n 使得 $\mathfrak{p}^n\,|\,\mathfrak{a}$，$\mathfrak{p}^{n+1}\nmid\mathfrak{a}$.（后者表示 $\mathfrak{p}^{n+1}$ 不整除 $\mathfrak{a}$）. 记这个 n 为 $\nu_{\mathfrak{p}}(\mathfrak{a})$.

(2) $\nu_{\mathfrak{p}}(\mathfrak{a}+\mathfrak{b})=\min(\nu_{\mathfrak{p}}(\mathfrak{a}),\nu_{\mathfrak{p}}(\mathfrak{b}))$，

$\nu_{\mathfrak{p}}(\mathfrak{a}\cap\mathfrak{b})=\max(\nu_{\mathfrak{p}}(\mathfrak{a}),\nu_{\mathfrak{p}}(\mathfrak{b}))$，

$\nu_{\mathfrak{p}}(\mathfrak{a}\mathfrak{b})=\nu_{\mathfrak{p}}(\mathfrak{a})+\nu_{\mathfrak{p}}(\mathfrak{b})$.

(3) $\mathfrak{a}=\prod_{(0)\neq\mathfrak{p}\in \operatorname{Spec}D}\mathfrak{p}^{\nu_{\mathfrak{p}}(\mathfrak{a})}$ (有限乘积).

4．设D为 Dedekind 整环，S为D的乘法集，$0\notin S$。如果$S^{-1}D$不是域，则$S^{-1}D$也是 Dedekind整环。

5．(1)证明代数数域 $K=\mathbf{Q}(\sqrt{10})$的代数整数环为$O_K=\mathbf{Z}[\sqrt{10}]$。

(2)证明 $\mathbf{Z}[\sqrt{10}]$不是主理想整环。

6．证明$\mathbf{Q}(\sqrt{-3})$的代数整数环为$\mathbf{Z}\left[\frac{1}{2}(1+\sqrt{-3})\right]$。

7．求证D的每个分式理想均可唯一地表示成两个互素整理想之商。

8．设R为整环。求证：R是 Dedekind整环$\Longleftrightarrow R$为Noether 整闭整环并且对R的每个非零理想 $\mathfrak{a}$，$R/\mathfrak{a}$ 均是 Artin 环。

9．设 $\mathfrak{a}$ 为D的非零整理想，求证$D/\mathfrak{a}$ 为主理想环。

10．求证D的每个分式理想均可由两个元素生成。

11．(中国剩余定理) 设 $\mathfrak{a}_1,\cdots,\mathfrak{a}_n$为$D$中的整理想，$a_1,\cdots,a_n\in D$。求证方程组

$$x\equiv a_i(\operatorname{mod}\mathfrak{a}_i)\quad(1\leqslant i\leqslant n)$$

在D中有解的充要条件是：对每组 $i,j(1\leqslant i<j\leqslant n)$，$a_i\equiv a_j(\operatorname{mod}\mathfrak{a}_i+\mathfrak{a}_j)$。
[提示：证明 D-模序列 $D\xrightarrow{\varphi}\bigoplus_{i=1}^{n}D/\mathfrak{a}_i\xrightarrow{\psi}\bigoplus_{1\leqslant i<j\leqslant n}D/(\mathfrak{a}_i+\mathfrak{a}_j)$ 是正合的，其中

$$\varphi(a)=(a+\mathfrak{a}_1,\cdots,a+\mathfrak{a}_n),\quad(a\in D)$$

$$\psi(a_1+\mathfrak{a}_1,\cdots,a_n+\mathfrak{a}_n)=(a_i-a_j+(\mathfrak{a}_i+\mathfrak{a}_j))_{1\leqslant i<j\leqslant n}\text{ .]}$$

12．设 $\mathfrak{a}$ 和 $\mathfrak{b}$ 分别是D的分式理想和整理想。求证存在 $0\neq a\in K$，使得 $a\mathfrak{a}+\mathfrak{b}=D$。

13．设M为有限生成扭D-模。

(1)对D的每个非零素理想$\mathfrak{p}$，求证$M_{\mathfrak{p}}=\{x\in M\mid$存在$n\geqslant0$使得$\mathfrak{p}^n x=(0)\}$是$M$的 D-子模。并且若 $\mathfrak{p}'$为D 的另一非零素理想，$\mathfrak{p}'\neq\mathfrak{p}$，则 $M_{\mathfrak{p}}\cap M_{\mathfrak{p}'}=(0)$。

(2)求证M唯一地表示成有限直和：$M=\bigoplus_{(0)\neq\mathfrak{p}\in\operatorname{Spec}D}M_{\mathfrak{p}}$

14．设R为整环，K为R的商域。$\mathfrak{a}$和$\mathfrak{b}$为R 的分式理想，$f:\mathfrak{a}\to\mathfrak{b}$是 R-模同态。求证存在$c\in K$使得 $f(a)=ca$(对每个$a\in\mathfrak{a}$)。于是f或为零同态或为单同态，特别地，$\mathfrak{a}\cong\mathfrak{b}$($R$-模同构)$\Longleftrightarrow$存在$0\neq c\in K$使得$\mathfrak{a}=c\mathfrak{b}$。

15．令$K=\mathbf{Q}(\sqrt{x-1})$，O_K为$\mathbf{Q}[x]$在域K中的整闭包。

(1)试决定O_K，并证明O_K是Dedekind整环。

(2)将O_K中理想$(x-2)O_K$分解成素理想之积

第六章　代数簇和代数整数环

为了避免使读者陷入空泛的概念之中，我们在这一章里介绍交换代数的背景性材料，即介绍代数几何与代数数论的初步知识．这里的介绍是粗浅的，对某些较深入的内容我们只作了某些描述性的论述，详细而充分的讨论则属于代数几何和代数数论专门范围．我们的目的主要是试图通过这些基本材料使大家了解到，交换代数这门学科起源于代数几何与代数数论的研究，并为这两门学科的深化提供了有效的工具，从而极大地促进了这两门学科的发展．

§6.1　代数集合与代数簇

先谈代数几何．设 k 为域，$f_i(x_1,\cdots,x_n)\in k[x_1,\cdots,x_n]$ $(1\leqslant i\leqslant m)$．代数几何的最基本问题是研究代数方程组

$$f_i(x_1,\cdots,x_n)=0\quad(1\leqslant i\leqslant m)\tag{1}$$

在域 k 中解的性质．如果 f_i 均是一次多项式，这就是线性方程组，我们有相当完整的解域上线性方程组的理论——线性代数．当 f_i 的次数大于 1 时，研究代数方程组(1)的解（如解的存在性，如何刻画全部解，如何将解集合作适当分类等）是很不简单的问题．例如考虑方程 $x^n+y^n=1$（n 为大于 2 的自然数，这是平面上一条代数曲线）．在实数域上我们不难把它的全部实数解用参数表达出来．但是在有理数域 Q 上考虑时，著名的 Fermat 猜想是说：此方程没有有理解 (x,y)，使得 $xy\neq0$．这个问题至今没有完全解决．对于多于一个方程的方程组，则难度就更大．在代数几何的早期研究中更多地借助于几何直观，主要研究 $n\leqslant3$ 的情形．同时，由于没有一般性方法和工具，结果也主要是涉及个别方程或相当特殊的方程组．自从 Noether 的理想准素分解理论和局部化

方法产生以后，代数几何的许多问题可以叙述得更为明确，同时也导致许多系统和深刻的结果．现在我们来展示代数几何是如何建立在交换代数理论基础之上的．

设 k 为域，S 为多项式环 $k[x_1,\cdots,x_n]$ 的一个子集合（可以是无限集合）．S 中所有多项式在域 k 中的公共根集合显然是

$V(S)=\{(a_1,\cdots,a_n)\in k^n \mid f(a_1,\cdots,a_n)=0,$
对每个 $f\in S\}$.

定义 域 k 上 n 维仿射空间 k^n 中的子集合 V 叫作（仿射）**代数集合**，是指存在某个多项式集合 $S\subseteq k[x_1,\cdots, x_n]$，使得 $V=V(S)$.

如果 $f,g\in S,h\in k[x_1,\cdots,x_n]$，则对每个点 $(a_1,\cdots,a_n)\in V(S)$，均有 $(f\pm g)(a_1,\cdots,a_n)=f(a_1,\cdots,a_n)\pm g(a_1,\cdots,a_n)=0$，$(hf)(a_1,\cdots,a_n)=h(a_1,\cdots,a_n)f(a_1,\cdots,a_n)=0$．因此，如果以 (S) 表示由集合 S 生成的 $k[x_1,\cdots,x_n]$ 中的理想，则 $V(S)=V((S))$．换句话说，k^n 中每个代数集合均可表示成 $V(\mathfrak{a})$，其中 $\mathfrak{a}$ 是 $k[x_1,\cdots,x_n]$ 的某个理想．我们称 $V(\mathfrak{a})$ 是**理想 $\mathfrak{a}$ 对应的代数集合**．由于 $k[x_1,\cdots,x_n]$ 是 Noether 环，从而它的每个理想都是有限生成的．设 $f_1,\cdots, f_m$ 是理想 $\mathfrak{a}$ 的一组生成元，则 $V(\mathfrak{a})=V((f_1,\cdots,f_m))$．于是代数集合 $V(\mathfrak{a})$ 是有限个多项式 $f_1,\cdots,f_m$ 在 k 上的公共根集合．所以象本节开头那样假定 S 是有限集合 $\{f_1,\cdots,f_m\}$ 是不失普遍性的．也就是说，k^n 中每个代数集合都是有限个代数方程组成的方程组(1)在 k 中解的全体，从而是代数几何的基本研究对象．

反过来，给了 k^n 中任意一个子集合 A，定义

$I(A)=\{f(x_1,\cdots,x_n)\in k[x_1,\cdots,x_n] \mid f(a_1,\cdots,a_n)=0,$
对每个 $(a_1,\cdots,a_n)\in A\}$.

换句话说，$I(A)$ 是以 A 中所有点为根的那些多项式全体．显然 $I(A)$ 是 $k[x_1, \cdots, x_n]$ 的一个理想，叫作是**点集 A 对应的多项**

式理想.

对应 $S\mapsto V(S)$和 $A\mapsto I(A)$之间有如下一些简单性质.

引理 1 设k为域,S,T,S_i均为$k[x_1,\cdots,x_n]$的子集合,A和B为k^n的子集合. 则

(1) $S\subseteq T\Rightarrow V(S)\supseteq V(T)$;$A\subseteq B\Rightarrow I(A)\supseteq I(B)$.

(2) $S\subseteq IV(S)$,$A\subseteq VI(A)$.

(3) $V(S)=VIV(S)$,$I(A)=IVI(A)$.

(4) $V(S_1\cap S_2\cap\cdots\cap S_n)\supseteq V(S_1)\cup V(S_2)\cup\cdots\cup V(S_n)$.
又若$S_1,\cdots,S_n$均是$k[x_1,\cdots,x_n]$的理想,则等式成立.

(5) $V(\bigcup_{i\in J}S_i)=\bigcap_{i\in J}V(S_i)$.

证明 (1),(2),(4),(5)由定义直接推出.

(3):由$S\subseteq IV(S)$和(1)中关系可知$V(S)\supseteq VIV(S)$. 另一方面,由(2),$V(S)\subseteq VI(V(S))=VIV(S)$,从而$V(S)=VIV(S)$. 同样可证$I(A)=IVI(A)$. ▌

注记 由引理1的(4)和(5),我们知道,k^n中有限个代数集合的并集和任意多个代数集合的交集仍然是代数集合,此外,空集$\varnothing=V(k[x_1,\cdots,x_n])$和整个仿射空间$k^n=V((0))$都是代数集合.

代数几何的结果以k是代数封闭域的情形最为完善.(一个域k叫作是**代数封闭的**,是指k的扩域中每个在k上代数的元素均属于k.)古典代数几何就是在代数封闭域C(复数域)上考虑问题. 今后在多数情形下,我们都假定k为代数封闭域.

例 1 我们决定仿射直线k(k为任意域)上的全部代数集合. 由于每个非零多项式$f(x)\in k[x]$在域k中至多有有限多解,所以除了k本身之外,其他代数集合均是有限集合. 另一方面,k的每个有限集合$\{a_1,\cdots,a_n\}$也必然是代数集合,因为它是多项式$f(x)=(x-a_1)\cdots(x-a_n)\in k[x]$的全部解. 从而仿射直线$k$的全部代数集合是:$k$和$k$的所有有限子集合(包括空集).

例 2 设 k 是代数封闭域. $f(x,y)$ 是 $k[x,y]$ 中的多项式并且 $\deg f\geqslant 1$. 我们以 $\deg f$ 表示 f 对于 x 和 y 的全次数, $\deg_y f$ 表示 f 对于 y 的次数(x 看作常量), 类似定义 $\deg_x f$. 显然 $\max(\deg_x f,\deg_y f)\leqslant\deg f\leqslant\deg_x f+\deg_y f$. 理想 (f) 对应的代数集合是 $V(f)=\{(a,b)\in k^2|f(a,b)=0\}$, 即方程 $f(x,y)=0$ 在域 k 中的全部解. 不妨设 $\deg_y f\geqslant 1$. 则 $f(x,y)=p_0(x)y^n+p_1(x)y^{n-1}+\cdots+p_n(x)$. $p_0(x)\neq 0, n\geqslant 1$. 由于 $p_0(x)$ 在 k 中只有有限多解, 而代数封闭域 k 必然是无限域, 因此存在无限多个 $a\in k$, 使得 $p_0(a)\neq 0$. 于是 $f(a,y)$ 是 y 的 n 次多项式 $(n\geqslant 1)$, 从而在代数封闭域 k 中必然有根. 即对于无限多个 $a\in k$, 均有 $b\in k$ 使得 $f(a,b)=0$, 从而代数集合 $V(f)$ 是无限集. $V(f)$ **称作是平面代数曲线**. 于是, 在代数封闭域上每个平面代数曲线均有无限多个点.

例 3 设 k 为代数封闭域, 我们现在来决定仿射平面 k^2 的全部代数集合. 设 $f_1(x,y),f_2(x,y)\in k[x,y]$. 如果 $(f_1,f_2)=1$ (注意 $k[x,y]$ 是唯一因子分解整环, 从而在其中有最大公因子概念). 我们现在来证明代数集合 $V(f_1,f_2)=\{(a,b)\in k^2|f_1(a,b)=f_2(a,b)=0\}$ 是有限集. 如果 $\deg_x f_1$ 或 $\deg_x f_2$ 为 0, 则 $V(f_1,f_2)$ 显然有限. 因此不妨设 $\deg_x f_1\geqslant\deg_x f_2\geqslant 1$. 于是可写为

$f_1=g_0(y)x^n+\cdots+g_n(y)$,

$f_2=h_0(y)x^m+\cdots+h_m(y)$. $g_0(y),h_0(y)\neq 0, n\geqslant m\geqslant 1$.

令 $h(x,y)=h_0(y)f_1(x,y)-g_0(y)f_2(x,y)x^{n-m}$, 则 $\deg_x h<n=\deg_x f_1$. 如果 $(a,b)\in V(f_1,f_2)$, 则 $h(a,b)=h_0(b)f_1(a,b)-g_0(b)f_2(a,b)a^{n-m}=0$. 如果仍然 $\deg_x h\geqslant\deg_x f_2$, 则可以继续作下去. 用类似于辗转相除的程序, 我们可以得到 $\tilde{h}(x,y)$, $\deg_x\tilde{h}=0$, 即 $\tilde{h}(x,y)=\tilde{h}(y)$, 使得 $\tilde{h}(a,b)=\tilde{h}(b)=0$. 由于 $(f_1,f_2)=1$, 可知 $\tilde{h}(y)$ 不是恒为 0 的多项式. 从而 $\tilde{h}(y)=0$ 只有有限多解. 于是 b 只有有限多种可能性. 类似地, a 也只有有限多种可能性. 于是 $V(f_1,f_2)$ 是有限集.

如果 $(f_1,f_2)=f(x,y)$，并且 $\deg f\geqslant 1$．令 $f_1=fg_1$，$f_2=fg_2$，则$(g_1,g_2)=1$．不难看出$V(f_1,f_2)=V(f)\cup V(g_1,g_2)$，前者是平面代数曲线，在例 2 中证明了它是无限集合，而后者是有限集合．完全类似地，对于任意有限个非零多项式 $f_i(x,y)\in k[x,y]$，$(1\leqslant i\leqslant m)$．令$(f_1,\cdots,f_m)=f$．如果 $\deg f\geqslant 1$，则 $V(f_1,\cdots,f_m)$是平面代数曲线$V(f)$和有限集合之并．如果$(f_1,\cdots,f_m)=1$，则 $V(f_1,\cdots,f_m)$为有限集合．由于 k^2 中每个有限集合均是代数集合(见下面例 4)，从而 k^2 中的全部代数集合是：k^2，平面代数曲线，有限集(包括空集)，以及平面代数曲线加上一个有限集合．

例 4 设 k 为任意域，$n\geqslant 1$．对于 k^n 中每个点$(a_1,\cdots,a_n)$，$a_i\in k$．方程组 $x_i-a_i=0(1\leqslant i\leqslant n)$ 的解恰好就是这一个点．于是 k^n 中每个一点集合均是代数集合．从而由引理 1 的 (4) 可知 k^n 中每个有限集合均是代数集合．特别当 k 为有限域时，k^n 中每个子集合均是代数集合．但是当 k 为无限域时，对于 $n\geqslant 3$，如何决定出 k^n 的全部无限代数集合，即使对代数封闭域都是代数几何的一个困难问题．

象以上诸例中所用的"手工"方法显然是不能走很远的．让我们继续作理论上的探讨．对于 $k[x_1,\cdots,x_n]$中每个理想 $\mathfrak{a}$，由引理 1 的(2)可知 $IV(\mathfrak{a})$ 是包含 $\mathfrak{a}$ 的理想．为了弄清这两个理想之间的联系，我们需要如下引理．

引理 2 设 k 为域，如果 $y_1,\cdots,y_n$ 是 k 的某个扩域中的元素，并且环 $F=k[y_1,\cdots,y_n]$ 为域，则每个 y_i 在 k 上均是代数的．

证明 当 $n=1$ 时这就是域论中的熟知结果．证明也极为简单：如果 $k[y]$ 是域，则$\frac{1}{y}\in k[y]$，从而$\frac{1}{y}$可以表成多项式形式$\frac{1}{y}=f(y)\in k[y]$，于是 y 就是非零多项式 $xf(x)-1$ 的根，即 y 是

k 上的代数元素．现在对 n 归纳．由于 F 是域，从而可以将 F 写成 $F=k(y_n)[y_1,\cdots,y_{n-1}]$，$k(y_n)$ 是 F 的子域．根据归纳假设，$y_1,\cdots,y_{n-1}$ 均在 $k(y_n)$ 上代数．如果我们能证明 y_n 在 k 上代数，那末 $y_1,\cdots,y_{n-1}$ 在 k 上便也是代数的，从而证明了引理．现在假设 y_n 不是 k 上代数元素，则 y_n 为 k 上超越元素．这时，多项式环 $k[y_n]$ 为主理想整环，从而为整闭整环．由于 $y_1,\cdots,y_{n-1}$ 均在 $k(y_n)$ 上代数，而 $k(y_n)$ 是 $k[y_n]$ 的商域，从而存在 $p(y_n)\in k[y_n]$，使得 $p(y_n)y_i(1\leqslant i\leqslant n-1)$ 均在 $k[y_n]$ 上整．现在对于任意有理函数 $g(y_n)\in k(y_n)$，由于 $k(y_n)\subseteq k[y_1,\cdots,y_n]$，于是有多项式 $f(y_1,\cdots,y_n)\in k[y_1,\cdots,y_n]$ 使得 $g(y_n)=f(y_1,\cdots,y_n)$．从而有充分大的 d（例如取 $d=\deg f$），使得多项式 $f(y_1,\cdots,y_n)$ 的每个单项式乘上 $p(y_n)^d$ 均在 $k[y_n]$ 上整．于是 $p(y_n)^d f(y_1,\cdots,y_n)$ 在 $k[y_n]$ 上整．但是 $p(y_n)^d f(y_1,\cdots,y_n)=p(y_n)^d g(y_n)\in k(y_n)$，而 $k[y_n]$ 是整闭整环，因此 $p(y_n)^d f(y_1,\cdots,y_n)\in k[y_n]$．令 $h(y_n)=p(y_n)^d g(y_n)$，则 $h(y_n)\in k[y_n]$，而 $g(y_n)=h(y_n)/p(y_n)^d$．这就是说，每个有理函数 $g(y_n)\in k(y_n)$ 均可表成关于 y_n 的两个多项式之商，其分母是一个固定多项式 $p(y_n)$ 的幂．这显然是不可能的（例如取 $g(y_n)=\dfrac{1}{1+p(y_n)}$，而 $\deg p(y_n)\geqslant 1$）．从而 y_n 必然在 k 上代数，于是完成了引理 2 的证明．▌

下一个定理对于代数几何是很基本的．

定理 1（Hilbert 零点定理） 设 k 是代数封闭域，$\mathfrak{a}$ 为 $k[x_1,\cdots,x_n]$ 的真理想，则 $V(\mathfrak{a})\neq\emptyset$．换句话说，对于多项式 $f_1,\cdots,f_m\in k[x_1,\cdots,x_n]$，如果 1 不属于 $f_1,\cdots,f_m$ 所生成的理想，则方程组 $f_i(x_1,\cdots,x_n)=0(1\leqslant i\leqslant m)$ 在代数封闭域 k 中必有解．

证明 由假设可知 $k[x_1,\cdots,x_n]$ 中存在极大理想 $\mathfrak{m}$ 包含 $\mathfrak{a}$．于是 $V(\mathfrak{m})\subseteq V(\mathfrak{a})$．从而我们只需证明 $V(\mathfrak{m})\neq\emptyset$ 即可．考虑域

$F=k[x_1,\cdots,x_n]/\mathfrak{m}=k[y_1,\cdots,y_n]$，其中 y_i 是 x_i 在 F 中的象．由于 $\mathfrak{m}\cap k=(0)$，从而 k 可看成是 F 的子域．根据引理 2 可知 $y_1,\cdots,y_n$ 均在 k 上代数．但是已假定 k 是代数封闭域，从而 $y_i\in k$，即 $F=k$．于是我们有域的同构 $\varphi: F=k[x_1,\cdots,x_n]/\mathfrak{m}\cong k$，并且对每个 $a\in k$，均有 $\varphi(a)=a$．令 $\varphi(y_i)=a_i\in k(1\leqslant i\leqslant n)$．则对每个 $f(x_1,\cdots,x_n)\in\mathfrak{m}$，$f$ 在 F 中的象 $\bar{f}=\bar{0}$．从而 $0=\varphi(\bar{f}(x_1,\cdots,x_n))=\varphi(f(y_1,\cdots,y_n))=f(a_1,\cdots,a_n)$．这就表明 $(a_1,\cdots,a_n)\in V(\mathfrak{m})$．即 $V(\mathfrak{m})\neq\varnothing$．▌

注记 如果 k 不是代数封闭域，则此定理不必正确．例如取 k 为实数域，而 $\mathfrak{a}=(x^2+1)$．

定义 设 k 为域．$k[x_1,\cdots,x_n]$ 中理想 $\mathfrak{a}$ 叫作是**根式理想**，是指 $\mathfrak{a}=\sqrt{\mathfrak{a}}$．

不难看出，$\mathfrak{a}$ 是根式理想 $\Longleftrightarrow$ $\mathfrak{a}$ 可唯一地表成有限个互相不包含的素理想之交．$\Big($$\Leftarrow$：若 $\mathfrak{a}=\bigcap_{i=1}^{n}\mathfrak{p}_i$，则 $\sqrt{\mathfrak{a}}=\bigcap_{i=1}^{n}\sqrt{\mathfrak{p}_i}=\bigcap_{i=1}^{n}\mathfrak{p}_i=\mathfrak{a}$．$\Rightarrow$：由于 $k[x_1,\cdots,x_n]$ 为 Noether 环，从而每个理想均有极小准素分解式 $\mathfrak{a}=\bigcap_{i=1}^{n}\mathfrak{q}_i$，$\mathfrak{p}_i=\sqrt{\mathfrak{q}_i}$．如果 $\mathfrak{a}$ 为根式理想，则 $\mathfrak{a}=\sqrt{\mathfrak{a}}=\bigcap_{i=1}^{n}\mathfrak{p}_i$．去掉全部嵌入素理想(比如是 $\mathfrak{p}_{m+1},\cdots,\mathfrak{p}_n$)之后，$\mathfrak{a}=\bigcap_{i=1}^{m}\mathfrak{p}_i$，其中 $\mathfrak{p}_i(1\leqslant i\leqslant m)$ 两两互不包含．由于 $\mathfrak{a}=\bigcap_{i=1}^{m}\mathfrak{p}_i$ 是极小准素分解式，并且没有嵌入准素分支．从而 $\{\mathfrak{p}_1,\cdots,\mathfrak{p}_m\}$ 是由 $\mathfrak{a}$ 所决定的．) 特别地，每个素理想均是根式理想．下面定理表明：对于代数封闭域 k，k^n 中代数集合与 $k[x_1,\cdots,x_n]$ 中根式理想是反序一一对应的．

定理 2 设 k 为代数封闭域，$\mathfrak{a}$ 为 $k[x_1,\cdots,x_n]$ 中的理想. 则

(1) $\mathfrak{a}=(0)\Longleftrightarrow V(\mathfrak{a})=k^n$，$\mathfrak{a}=k[x_1,\cdots,x_n]\Longleftrightarrow V(\mathfrak{a})=\varnothing$.

(2) $IV(\mathfrak{a})=\sqrt{\mathfrak{a}}$.

(3) 令 $\mathscr{A}$ 为 k^n 中代数集合全体，$\mathscr{R}$ 为 $k[x_1,\cdots,x_n]$ 中根式理想全体，则映射

$I:\mathscr{A}\mapsto\mathscr{R}, S\mapsto I(S), V:\mathscr{R}\mapsto\mathscr{A}, \mathfrak{a}\mapsto V(\mathfrak{a})$

是集合 $\mathscr{A}$ 与 $\mathscr{R}$ 之间互逆的反序一一对应.

证明 (1) $V(\mathfrak{a})=k^n\Rightarrow\mathfrak{a}=(0)$：当 $n=1$ 时这显然正确. 因为 k 是无限域，而如果 $\mathfrak{a}$ 中有非零多项式则 $V(\mathfrak{a})$ 只能是有限集. 现在对 n 归纳. 设 $0\neq f(x_1,\cdots,x_n)\in\mathfrak{a}$. 记 $f=g_0(x_1,\cdots,x_{n-1})x_n^m+\cdots+g_m(x_1,\cdots,x_{n-1})$，$g_0\neq0$. 根据归纳假设，存在 $(a_1,\cdots,a_{n-1})\in k^{n-1}$ 使得 $g_0(a_1,\cdots,a_{n-1})\neq0$. 于是 $f(a_1,\cdots,a_{n-1},x_n)$ 是 x_n 的 m 次多项式，从而必有 $a_n\in k$，使得 $f(a_1,\cdots,a_{n-1},a_n)\neq0$. 即 $V(\mathfrak{a})\subseteq V(f)\neq k^n$. 因此若 $V(\mathfrak{a})=k^n$，则 $\mathfrak{a}=(0)$.

$V(\mathfrak{a})=\varnothing\Rightarrow\mathfrak{a}=k[x_1,\cdots,x_n]$ 即是 Hilbert 零点定理. 而另两个论断则是显然的.

(2) 设 $f\in\sqrt{\mathfrak{a}}$，则有 $m\geqslant1$ 使得 $f^m\in\mathfrak{a}$. 从而对每个 $(a_1,\cdots,a_n)\in V(\mathfrak{a})$ 均有 $f^m(a_1,\cdots,a_m)=0$. 于是 $f(a_1,\cdots,a_m)=0$(因为 k 是域). 因此 $f\in IV(\mathfrak{a})$. 即 $\sqrt{\mathfrak{a}}\subseteq IV(\mathfrak{a})$. 为证 $IV(\mathfrak{a})\subseteq\sqrt{\mathfrak{a}}$，我们只需证明若 $0\neq f\in IV(\mathfrak{a})$，则有 m 使得 $f^m\in\mathfrak{a}$.

考虑 $k[x_1,\cdots,x_n,x_{n+1}]$ 中的理想 $\mathfrak{b}=(\mathfrak{a},1-x_{n+1}f(x_1,\cdots,x_n))$. (即是集合 $\mathfrak{a}\cup\{1-x_{n+1}f(x_1,\cdots,x_n)\}$ 在 $k[x_1,\cdots,x_{n+1}]$ 中生成的理想.) 如果 $(a_1,\cdots,a_{n+1})\in V(\mathfrak{b})$，则 $(a_1,\cdots,a_n)\in V(\mathfrak{a})$，从而 $1-a_{n+1}f(a_1,\cdots,a_n)=1-0=1\neq0$. 即 $(a_1,\cdots,a_{n+1})$ 不是 $1-x_{n+1}f(x_1,\cdots,x_n)=0$ 的解. 这一矛盾表明 $V(\mathfrak{b})=\varnothing$. 于是由 Hilbert 零点定理可知 $\mathfrak{b}=k[x_1,\cdots,x_{n+1}]$. 从而 $1\in\mathfrak{b}$，即

$$1=\sum_{j=1}^{t} r_j q_j + r(1-x_{n+1}f),$$

其中 $q_j(x_1,\cdots,x_n)\in\mathfrak{a}$, $r_j(x_1,\cdots,x_{n+1})$, $r(x_1,\cdots,x_{n+1})\in k[x_1,\cdots,x_{n+1}]$. 取 $x_{n+1}=1/f$,则 $1=\sum_{j=1}^{t}\bar{r}_j q_j$, $\bar{r}_j\in k\left[x_1,\cdots,x_n,\frac{1}{f}\right]$, 通分后对充分大的 m 则可使

$$f^m=\sum_{j=1}^{t}(f^m\bar{r}_j)q_j,\quad f^m\bar{r}_j\in k[x_1,\cdots,x_n].$$

由于 $q_j\in\mathfrak{a}(1\leqslant j\leqslant t)$,从而 $f^m\in\mathfrak{a}$.

(3) 对于每个 $S\in\mathscr{A}$, 则有理想 $\mathfrak{a}$ 使得 $S=V(\mathfrak{a})$, 于是 $VI(S)=VIV(\mathfrak{a})=V(\mathfrak{a})=S$. 另一方面,对每个 $\sqrt{\mathfrak{a}}=\mathfrak{a}\in\mathscr{R}$, 有 $IV(\sqrt{\mathfrak{a}})=\sqrt{\sqrt{\mathfrak{a}}}=\sqrt{\mathfrak{a}}$. 反序是由于引理 1 的(1). ∎

注记 与公式 $IV(\mathfrak{a})=\sqrt{\mathfrak{a}}$ 相对应的,对于每个子集合 $S\subseteq k^n$,可以证得 $VI(S)=\bar{S}$, 其中 $\bar{S}$ 是包含 S 的最小的代数集合.

定义 k^n 中代数集合 V 叫作是不可约的, 是指 k^n 中不存在代数集合 V_1,V_2,使得 $V\supset V_1,V\supset V_2,V=V_1\cup V_2$. (即 V 不是两个真子集之并,而这两个真子集也是代数集合.)否则称代数集合可约. 不可约代数集合也叫作是代数簇.

定理 3 设 k 是代数封闭域. $R=k[x_1,\cdots,x_n],n\geqslant 1$.

(1) k^n 中代数集合 A 是代数簇 $\Longleftrightarrow I(A)$ 为 R 的素理想.

(2) 每个代数集合均可唯一地表示成有限个彼此不相互包含的代数簇之并.

(3) 令 $\mathscr{U}$ 为 k^n 中的代数簇全体,则

$I:\mathscr{U}\mapsto \operatorname{Spec}R,\ A\mapsto I(A)$,

$V:\operatorname{Spec}R\mapsto\mathscr{U},\ \mathfrak{p}\mapsto V(\mathfrak{p})$

是集合 $\mathscr{U}$ 与Spec$R$ 之间的反序一一对应.

证明 (1)和(2):设A为代数集合,则有R的根式理想 $\mathfrak{a}$ 使得 $A=V(\mathfrak{a}),\mathfrak{a}=I(A)$. 但是 $\mathfrak{a}=\bigcap_{i=1}^{m}\mathfrak{p}_i$,其中 $\mathfrak{p}_i$ 是两两彼此不相包含的素理想.对应有 $A=V(\mathfrak{a})=\bigcup_{i=1}^{m}V(\mathfrak{p}_i)$,其中$V(\mathfrak{p}_i)$是两两不相包含的代数集合. 于是若 $\mathfrak{a}$ 不为素理想,则 $m\geqslant 2$. 从而A是可约的. 反之若 $\mathfrak{a}$ 为素理想. 如果 $A=A_1\cup A_2$,其中 A_1 和 A_2 为代数集合. 令 $\mathfrak{a}_1=I(A_1),\mathfrak{a}_2=I(A_2)$,则 $\mathfrak{a}=I(A)=I(A_1)\cap I(A_2)=\mathfrak{a}_1\cap\mathfrak{a}_2$. 由于 $\mathfrak{a}$ 是素理想, 从而 $\mathfrak{a}=\mathfrak{a}_1$或者 $\mathfrak{a}=\mathfrak{a}_2$. 即 $A=A_1$或者 $A=A_2$. 从而当 $\mathfrak{a}$ 为素理想时, $A=V(\mathfrak{a})$是代数簇. 而对任意的根式理想 $\mathfrak{a}=\bigcap_{i=1}^{m}\mathfrak{p}_i,A=V(\mathfrak{a})$是有限个代数簇 $V(\mathfrak{p}_i)$ 的并集. 若 $\mathfrak{p}_i$ 两两不包含,则$\{\mathfrak{p}_1,\cdots,\mathfrak{p}_m\}$由 $\mathfrak{a}$ 唯一决定. 这时 $V(\mathfrak{p}_i)$也彼此不包含,并且代数簇 $V(\mathfrak{p}_i)(1\leqslant i\leqslant m)$也由 $A=V(\mathfrak{a})$ 所唯一决定.

(3) 由(1)和(2)立即得出. ▌

注记 (1)根据以上两个定理. 我们把 k^n 中代数集合这个代数几何的基本对象与 $k[x_1,\cdots,x_n]$ 中根式理想这一代数对象反序一一对应. 每个代数集合唯一地表示成有限个彼此不相包含的代数簇之并,而代数簇与 $k[x_1,\cdots,x_n]$ 中素理想反序一一对应. 所以最后化成一个提法简单的代数问题:决定多项式环 $R=k[x_1,\cdots,x_n]$的素谱 Spec$R$!

(2) 对于 $k[x_1,\cdots,x_n]$中任意理想 $\mathfrak{a}$,设 $\mathfrak{a}=\bigcap_{i=1}^{m}\mathfrak{q}_i$ 为极小准素分解式, $\mathfrak{p}_i=\sqrt{\mathfrak{q}_i}$,则 $V(\mathfrak{q}_i)=V(\sqrt{\mathfrak{q}_i})=V(\mathfrak{p}_i)$. 从而 $V(\mathfrak{a})=\bigcup_{i=1}^{m}V(\mathfrak{q}_i)=\bigcup_{i=1}^{m}V(\mathfrak{p}_i)$. 如果 $\mathfrak{p}_1\subset\mathfrak{p}_2$. 即 $\mathfrak{p}_2$是属于 $\mathfrak{a}$ 的嵌入素理

想，则 $V(\mathfrak{p}_1)\supset V(\mathfrak{p}_2)$. 换句话说，代数簇 $V(\mathfrak{p}_2)$ 包含在（或者说嵌在）代数簇 $V(\mathfrak{p}_1)$ 之中. 这就是我们将这种 $\mathfrak{p}_2$ 称作是属于 $\mathfrak{a}$ 的"嵌入"素理想的几何背景.

例 5 设 k 为代数封闭域. 回到§4.1的例子：$\mathfrak{a}=(x_1^2, x_1x_2)$ 为 $k[x_1,x_2]$ 中的理想. $\mathfrak{a}=\mathfrak{p}_1\cap\mathfrak{p}_2^2$ 是极小准素分解，其中 $\mathfrak{p}_1=(x_1)$，$\mathfrak{p}_2=(x_1,x_2)$. 于是 $V(\mathfrak{a})=V(\mathfrak{p}_1)\cup V(\mathfrak{p}_2)$，其中 $V(\mathfrak{p}_1)=\{(0,a)\in k^2 | a\in k\}$ 是 k^2 中一条仿射直线，而 $V(\mathfrak{p}_2)=\{(0,0)\}$ 为 k^2 的坐标原点，$V(\mathfrak{p}_2)$ 嵌在代数簇 $V(\mathfrak{p}_1)$ 之中，这是由于 $\mathfrak{p}_2\supset\mathfrak{p}_1$，即 $\mathfrak{p}_2$ 为属于 $\mathfrak{a}$ 的嵌入素理想.

例 6 设 k 为任意域，则 k^n 中每个一点集 $\{P=(a_1,\cdots,a_n)\}$ 均是最小的非零代数簇. 如果 k 是代数封闭域，我们由定理3中反序一一对应关系，可知 $\mathfrak{m}_P=I(\{P\})=(x_1-a_1,\cdots,x_n-a_n)$ 是 $k[x_1,\cdots,x_n]$ 中的极大理想. 并且每个极大理想均为这种形式. 所以对于代数封闭域 k，多项式环 $k[x_1,\cdots,x_n]$ 的极大谱有很简单的形式：$\mathrm{Max}\,k[x_1,\cdots,x_n]=\{\mathfrak{m}_P | P \text{ 为 } k^n \text{ 中一点}\}$.

习　题

（k 均指代数封闭域）

1. 设 $V_i(i=1,2,\cdots)$ 为 k^m 中代数集合. $V_1\supseteq V_2\supseteq\cdots\supseteq V_n\supseteq\cdots$，则必存在 n_0 使得 $V_{n_0}=V_{n_0+1}=\cdots$.

2. 如果域 K 不是代数封闭的，试问

(1) Hilbert 零点定理是否成立？

(2) 对于 $K[x_1,\cdots,x_n]$ 中每个理想 $\mathfrak{a}$，是否 $IV(\mathfrak{a})=\sqrt{\mathfrak{a}}$？

(3) $K[x_1,\cdots,x_n]$ 中极大理想是否均表成形式 $\mathfrak{m}=(x_1-a_1,\cdots,x_n-a_n)(a_i\in K)$？

3. 无限多个代数集合的并是否为代数集合？

4. 下列哪些是代数集合？

(1) $\{(t,t^2,t^3)\in k^3 | t\in k\}$.

(2) $\{(\cos t,\sin t)\in \mathbf{R}^2 | t\in \mathbf{R}\}$($\mathbf{R}$ 为实数域).

(3) $\{(r,\theta)\in \mathbf{R}^2 | r=\sin\theta\}$.

(4) $\{(x,y)\in \mathbf{C}^2 | |x|^2+|y|^2=1\}$. $\mathbf{C}$ 为复数域.

5. 设$(a_1^{(i)},\cdots,a_n^{(i)})\in k^n(1\leqslant i\leqslant m)$为$k^n$中$m$个不同的点. 求证存在多项式$f_i(x_1,\cdots,x_n)\in k[x_1,\cdots,x_n]$使得

$$f_j(a_1^{(i)},\cdots,a_n^{(i)})=\delta_{ij}，其中\delta_{ij}=\begin{cases}0, i\neq j时\\1, i=j时.\end{cases}$$

6. 对于$k[x,y,z]$中的理想$\mathfrak{a}=(x^2,xy,xz,yz)$,将$k^3$中代数集合$V(\mathfrak{a})$分解成彼此不包含的一些代数簇之并.

7. 设F为无限域. 求证$\{(a_1,\cdots,a_n)\in F^n | a_1a_2\cdots a_n\neq 0\}$不是代数集合.

8. 设F为域. V和W分别是F^n和F^m中代数集合. 求证$V\times W$为F^{n+m}中代数集合.

9. 决定Spec$k[x,y]$和Max$k[x,y]$.

§6.2 交换代数

我们在本书前言中申明：本课程是以交换环为主要研究对象的一门学科. 事实上，本书的前几章也完全以交换环作为研究对象. 可是本课程的名称却叫作"交换代数". 那是因为在代数几何中除了交换环之外,还需要再稍微复杂一点的代数结构,即环上的代数.

定义 设R是具有幺元素的交换环,一个 **R-代数**(或称**R上的代数**)是指满足以下条件的一个集合A.

(1) $(A,+,\cdot)$是环(通常环A不必交换也不必有幺元素)

(2) $(A,+)$是R-模.

(3) 对于$r\in R,a,b\in A$,均有$r(ab)=(ra)b=a(rb)$.

如果R-代数A本身是具有幺元素1_A的交换环，则称A是R上的**交换代数**. 不交换的R-代数在群表示理论等许多领域有重

要应用，形成代数学的一个分支．但是在本书中只涉及交换代数．

R-代数A叫作是**有限生成的**，是指存在有限个元素$a_1,\cdots,a_n\in A$，使得$A=R[a_1,\cdots,a_n]$．事实上，本章只涉及域k上有限生成的代数A，并且k是A的子域．

注记 有限生成R-代数A和有限生成R-模A不是一回事．例如多项式环$R[x]$为有限生成R-代数．但作为R-模$R[x]$不是有限生成的．

我们举一些R-代数的例子．

例 1 每个环(不必有幺元素也不必交换)均是Z-代数．

例 2 若$R\subseteq S$是环的扩张，其中R为具有幺元素的交换环，并且R中每个元素r与S中每个元素s均可交换，(即$rs=sr$)，则S是R-代数，其中所有的运算均是环S中的运算，比如每个具有幺元素的交换环R均是R-代数．R上的多项式环$R[x_1,\cdots,x_n]$和形式幂级数环$R[[x_1,\cdots,x_n]]$均是R-代数．

例 3 设R为具有幺元素的交换环，以$\mathrm{Mat}_n(R)$表示元素属于R的全体n阶方阵形成的矩阵环．事实上它是R-代数($r\cdot(a_{ij})=(ra_{ij})$)．并且当$n\geqslant 2$时，熟知这不是交换代数．

例 4 R如上，M为R-模，环$\mathrm{Hom}_R(M,M)$事实上是R-代数．在多数情形下这也不是交换代数．研究这个R-代数的结构是“结合代数”这门学科中的一个基本问题．

例 5 设G为乘法群，R如上所述，考虑集合

$$R[G]=\left\{\sum_{g\in G}r_g\cdot g\mid r_g\in R,\text{并且只有有限多个 } r_g \text{ 不为 } 0\right\}.$$

在$R[G]$上定义加法和乘法：

$$\sum_{g\in G}r_g g\pm\sum_{g\in G}s_g g=\sum_{g\in G}(r_g\pm s_g)g;$$

$$\Big(\sum_{g\in G} r_g g\Big)\Big(\sum_{g\in G} s_g g\Big)=\sum_{g\in G} t_g\cdot g,\ \text{其中}\ t_g=\sum_{h\cdot h'=g} r_h\cdot s_{h'}.$$

不难验证 $R[G]$对于这些运算形成环，它具有幺元素 $1_R\cdot e$，其中 e 为群 G 的单位元素，如果 G 为交换群，则 $R[G]$是交换环．再定义

$$r\cdot\sum_{g\in G} r_g\cdot g=\sum_{g\in G}(rr_g)\cdot g\quad\Big(r\in R,\ \sum_{g\in G} r_g\cdot g\in R[G]\Big).$$

则$R[G]$为 R-模，并且可直接验证 $R[G]$为 R-代数，如果 G 为交换群，则 $R[G]$是 R 上的交换代数，通常称 $R[G]$是群 G 在环 R 上的**群代数**．群代数 $R[G]$的结构与群 G 在环 R 上的表示理论有着直接的联系．

定义 设 R 为具有幺元素的交换环，A,B 为 R-代数．

(1) A 的子集合 A'叫作是 A 的**子代数**，是指 A'本身对于 A 中的运算是 R-代数．(即：A'是 A 的子环同时是 A 的 R-子模．)

(2) 映射 $f:A\to B$ 叫作是 R-**代数同态**，是指 f 为环同态同时也是 R-模同态，类似地定义 R-代数同构．

注记 (1) 如果 R-代数 A 有幺元素 1_A．则映射

$$f:R\to A,r\mapsto r\cdot 1_A$$

是 R-代数同态，如果 f 为单射，则我们通过 f 可把 R 看成是 A 的子代数．这时，$f(1_R)=1_R\cdot 1_A=1_A$．并且今后我们把 1_R 和 1_A 均写成 1．

(2) 设 A 和 B 为 R-代数，并且 R 为 A 和 B 的子代数．$1_R=1_A=1_B$．如果 $f:A\to B$ 是 R-代数同态，则作为环同态，我们总是假定 $f(1_A)=1_B$．于是对每个 $r\in R$，$f(r)=f(r\cdot 1_A)=rf(1_A)=r\cdot 1_B=r$．即 f 在 R 上的限制是恒等映射．

例 设 K 为域，V 为 K 上 n 维向量空间，取定 V 的一组基之后，每个 V 上的线性变换 $\varphi\in \mathrm{Hom}_K(V,V)$对于这组基均可表成一

个 n 阶方阵 $M_\varphi \in \mathrm{Mat}_n(K)$. 并且 $\varphi\pm\psi,\varphi\psi,a\varphi(a\in K)$分别对应方阵 $M_\varphi\pm M_\psi, M_\varphi M_\psi$ 和 aM_φ,于是我们有 K-代数同态: $\mathrm{Hom}_K(V,V)\to\mathrm{Mat}_n(K),\varphi\mapsto M_\varphi$. 事实上熟知这是 K-代数同构.

我们今后所需的关于 R-代数的知识仅此而已.

习　题

(A 均指环 R 上的代数)

1. A 的子集 I 如果既是 A 的 R-子模又是环 A 的理想,则称 I 是 A 的**代数理想**.(1) 对于 R-代数 A 的代数理想 I,试赋予 A/I 自然的商代数结构.

(2) 叙述并证明 R-代数的同态基本定理.

2. 设 A 为有理数域 $\mathbf{Q}$ 上的一维向量空间,定义 $ab=0$ (对任意 $a,b\in A$). 求证 A 为 $\mathbf{Q}$-代数. 对于 A 的每个加法子群 $0\neq I\neq A$, I 是环 A 的理想,但不是 A 的代数理想.

3. 设 A 有幺元素,求证环 A 的每个理想均是 R-代数 A 的代数理想.

4. R-代数 A 叫作是**平坦的**,是指 A 为平坦 R-模.

设 B 和 A 均为具有幺元素的交换环,并且 B 为平坦的 A-代数. 如果 M 为平坦 B-模,求证 M 也为平坦 A-模.

5. 设 A 和 B 均为 R-代数(R 为有幺元素的交换环). 在 R-模 $A\otimes_R B$ 中定义 $(a\otimes b)(a'\otimes b')=aa'\otimes bb'(a,a'\in A,b,b'\in B)$,并且由分配律将此乘法扩充到整个 $A\otimes_R B$ 之上. 求证由此使 $A\otimes_R B$ 成为 R-代数,称作是 **R-代数 A 和 B 的张量积**. 如果 A 本身也是具有幺元素的交换环,则 $A\otimes_R B$ 是 A-代数. (系数环的扩充)

6. 设 A,A',B,B' 均为 R-代数, $f:A\to B$, $f':A'\to B'$ 是 R-代数同态. 求证在模论中定义的 R-模同态 $f\otimes f':A\otimes_R A'\to B\otimes_R B'$ 事实上为 R-代数同态.

§ 6.3　同构和双有理同构

我们已经介绍了代数几何的基本对象——代数集合和代数

簇，下一步自然要研究它们之间的联系（适当的映射）和分类．设 k 是代数封闭域，V 为 k^n 中的代数集合，$\mathfrak{a}$ 是 V 所对应的根式理想．对于每个多项式 $f(x_1,\cdots,x_n)\in k[x_1,\cdots,x_n]$，考虑映射

$$f(x_1,\cdots,x_n):V\mapsto k,(a_1,\cdots,a_n)\mapsto f(a_1,\cdots,a_n).$$

问题在于：$k[x_1,\cdots,x_n]$ 中不同的多项式在看作是 V 上的函数时，可能是同一个函数．事实上，对于 $f,g\in k[x_1,\cdots,x_n]$，

$$f,g \text{ 为 } V \text{ 上的同一个函数} \Longleftrightarrow \text{对每个}(a_1,\cdots,a_n)\in V,$$
$$f(a_1,\cdots,a_n)-g(a_1,\cdots,a_n)=0$$
$$\Longleftrightarrow f-g\in I(V)=\mathfrak{a}.$$

从而 V 到 k 的一个多项式函数相当于商环 $k[x_1,\cdots,x_n]/\mathfrak{a}$ 的一个元素（等价类）．我们称 $k[x_1,\cdots,x_n]/\mathfrak{a}$ 为**代数集合 V 的（仿射）坐标环或多项式函数环**，表示成 $k[V]$．

我们不考虑 $V=\varnothing$ 的情形．当 $V\neq\varnothing$ 时，$\mathfrak{a}$ 是 $k[x_1,\cdots,x_n]$ 的真理想，从而 $\mathfrak{a}\cap k=(0)$．于是 k 可看成是 $k[V]=k[x_1,\cdots,x_n]/\mathfrak{a}$ 的子域．以 u_i 表示 x_i 在 $k[V]$ 中的象．则 $k[V]=k[u_1,\cdots,u_n]$．从而 $k[V]$ 是有限生成 k-代数．进而，$k[V]$ 中只有 0 是幂零元素．因为若 $f\in k[x_1,\cdots,x_n]$，$\bar{f}^n=\bar{0}\in k[V]$，则 $f^n\in\mathfrak{a}$．由于 $\mathfrak{a}$ 为根式理想，从而 $f\in\mathfrak{a}$，即 $\bar{f}=\bar{0}\in k[V]$，反过来，如果 Γ 包含 k 作为子域，并且

（1）Γ 是有限生成 k-代数；

（2）Γ 中没有非零的幂零元素．

则由（1）知有 $u_1,\cdots,u_n\in\Gamma$，使得 $\Gamma=k[u_1,\cdots,u_n]$．于是有环的满同态

$$\varphi:k[x_1,\cdots,x_n]\rightarrow k[u_1,\cdots,u_n],$$

使得 $\varphi(x_i)=u_i(1\leqslant i\leqslant n)$，并且 φ 在 k 上为恒等映射．令 $\mathfrak{a}=\mathrm{Ker}\varphi$．由条件（2）可知 $\mathfrak{a}=\sqrt{\mathfrak{a}}$．于是 $\mathfrak{a}$ 是 $k[x_1,\cdots,x_n]$ 的根式理想．从而有环的同构（事实上是 k-代数同构）

$$\Gamma=k[u_1,\cdots,u_n]\cong k[x_1,\cdots,x_n]/\mathfrak{a}$$

令$V=V(\mathfrak{a})\subseteq k^n$，则由$\mathfrak{a}\cap k=(0)$知$V\neq\varnothing$，并且$k[V]\cong\Gamma$（$k$-代数同构）．于是，代数集合的坐标环和具有性质(1)和(2)的k上的交换代数是相对应的．

例 1　设V为一点，$V=\{P\}$，$P=(a_1,\cdots,a_n)\in k^n$，则$V$对应的根式理想为极大理想$\mathfrak{m}_P=(x_1-a_1,\cdots,x_n-a_n)$．而$k[V]=k[x_1,\cdots,x_n]/\mathfrak{m}_P\cong k$．

例 2　设$V=k^n$，则$\mathfrak{a}=I(V)=(0)$，而$k[V]=k[x_1,\cdots,x_n]$．这说明在整个仿射空间k^n中（k代数封闭），不同的多项式即为不同的函数．

例 3　设V是仿射平面k^2中的双曲线$xy=1$，则它对应的根式理想为$\mathfrak{a}=(xy-1)$．从而$k[V]=k[x,y]/(xy-1)\cong k\left[x,\frac{1}{x}\right]=\left\{\frac{f(x)}{x^n}\,\middle|\,f(x)\in k[x],n\in\mathbf{Z}\right\}$．

如果代数集合V是k^n中的代数簇（k代数封闭），则V对应的根式理想为$k[x_1,\cdots,x_n]$的素理想$\mathfrak{p}$，从而V的坐标环$k[x_1,\cdots,x_n]/\mathfrak{p}=k[V]$是整环，它的商域称作是**代数簇$V$的有理函数域**，表示成$k(V)$．于是，$k(V)$中元素即是两个$V$上多项式函数之商（分母不恒为0），叫作是**$V$上的有理函数**．由于分母在$V$的某点可能取值为0，因此$V$上一个有理函数在$V$的某些点可能是没有定义的．

例　对于前面的例2（$V=k^n$），则$k(V)=k(x_1,\cdots,x_n)$，即是通常的有理函数域，对于前面的例3（V为双曲线$xy=1$），$k(V)\cong k(x)$．

现在研究代数集合或代数簇之间的映射．

定义　设V和W分别为k^n和k^m中的代数集合．对于多项式$f_i(x_1,\cdots,x_n)\in k[x_1,\cdots,x_n]$ $(1\leqslant i\leqslant m)$，我们有映射：

$$f=(f_1,\cdots,f_m):k^n\to k^m,$$

$$(a_1,\cdots a_n)\mapsto(f_1(a_1,\cdots,a_n),\cdots,f_m(a_1,\cdots,a_n)).$$

如果$f(V)\subseteq W$，我们就称f在V上的限制$f:V\to W$是从V到W的一个**多项式映射**. 由定义不难看出：

(1) 如果又有多项式映射$g:W\to U$，其中U是k^l中的代数集合，则$g\circ f:V\to U$也是多项式映射. 这是因为多项式与多项式的复合函数仍是多项式，并且$g\circ f(V)\subseteq g(W)\subseteq U$.

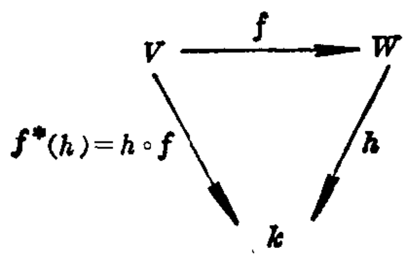
(2) $1_V:V\to V$是多项式映射. 这是由于$1_V=(x_1,\cdots,x_n)$. 即$f_i(x_1,\cdots,x_n)=x_i$ $(1\leqslant i\leqslant n)$.

定义 如果$f:V\to W$和$g:W\to V$是代数集合之间的多项式映射，并且$f\circ g=1_W$，$g\circ f=1_V$. 则称V和W是**同构的代数集合**. 如何将代数集合作同构分类，是代数几何一个基本问题. 现在我们把它化成代数问题.

设k为代数封闭域. $f:V\to W$为代数集合之间的多项式映射，$V\subseteq k^n$，$W\subseteq k^m$. 对于每个多项式函数$h(x_1,\cdots,x_m):W\to k$，我们得到多项式函数$h\circ f:V\to k$. 于是由f诱导出一个映射

$$f^*:k[W]\to k[V],\ f^*(h)=h\circ f.$$

这可表示成如下的交换图表



以下假设V和W均不是空集. 这时$\mathfrak{a}=I(V)$和$\mathfrak{b}=I(W)$分别是$k[x_1,\cdots,x_n]$和$k[y_1,\cdots,y_m]$中的真理想. 从而$k[V]$和$k[W]$均是k-代数，并且包含k作为子代数. 这时如果把k中元素a看作是$k[W]$中元素，即指是将W中所有点均映成a的多项式映射. 显然$f^*(a)=a$. 这表明f^*在k上的限制是恒等映射. 进而，不难看出$f^*(h_1\pm h_2)=f^*(h_1)\pm f^*(h_2)$，$f^*(h_1h_2)=f^*(h_1)$

$f^*(h_2)$. 因此 $f^*: k[W]\to k[V]$是 k-代数同态.

由定义可直接得到:

(1) 如果又有 $g: W\to U$ 为多项式映射,则$(g\circ f)^*=f^*\circ g^*: k[U]\to k[V]$.

(2) $(1_V)^*=1_{k[V]}$.

于是,若V和W是同构的代数集合,即存在多项式映射$f: V\to W$和 $g: W\to V$,使得 $g\circ f=1_V$, $f\circ g=1_W$. 则由上述两个性质可知 $f^*\circ g^*=(g\circ f)^*=(1_V)^*=1_{k[V]}$, 同样地, $g^*\circ f^*=1_{k[W]}$. 因此我们有 k-代数同构: $f^*: k[W]\simeq k[V]$.

反之,设 $\varphi: k[W]\to k[V]$是 k-代数同态. 考虑多项式函数 $y_i\in k[W]$, 则由 φ 给出多项式函数 $\varphi(y_i)=f_i(x_1,\cdots,x_n)\in k[V]$. 于是我们有映射

$$f=(f_1,\cdots,f_m): k^n\to k^m,$$

$$(a_1,\cdots,a_n)\mapsto(f_1(a_1,\cdots,a_n),\ \cdots,f_m(a_1,\cdots,a_n)).$$

对于每个 $h(y_1,\cdots,y_m)\in\mathfrak{b}=I(W)$, $h(y_1,\cdots,y_m)$ 作为 $k[W]$中的元素为 0. 由于 φ 为 k-代数同态,从而 $\varphi(h)(x_1,\cdots,x_n)=h(f_1(x_1,\cdots,x_n),\cdots,f_m(x_1,\cdots,x_n))$作为 $k[V]$中的元素也为 0, 即 $\varphi(h)\in\mathfrak{a}=I(V)$. 这就表明: 如果 $(a_1,\cdots,a_n)\in V$, 则 $h(f_1(a_1,\cdots,a_n),\cdots,f_m(a_1,\cdots,a_n))=0$, 对每个 $h(y_1,\cdots,y_m)\in\mathfrak{b}$ 均是如此. 从而$(f_1(a_1,\cdots,a_n),\cdots,f_m(a_1,\cdots,a_n))\in W$. 于是我们证得 $f(V)\subseteq W$. 即 f 是从V到W的多项式映射,并且对每个 $h(y_1,\cdots,y_m)\in k[W]$, $f^*(h)(x_1,\cdots,x_n)=h(f_1(x_1,\cdots,x_n),\cdots,f_m(x_1,\cdots,x_n))=\varphi(h)(x_1,\cdots,x_n)$. 从而 $f^*=\varphi$. 换句话说,对于每个 k-代数同态 $\varphi: k[W]\to k[V]$, 均存在多项式映射 $f: V\to W$,使得 $\varphi=f^*$.

最后,若 φ 是 $k[W]$上的恒等映射,则由上面方法构作出的 f 也是V上的恒等映射. 从而若 $\varphi: k[W]\to k[V]$是 k-代数同构,则对应得到的 $f: V\to W$ 也是代数集合的同构. 综合上述我们就

证得了如下的定理.

定理 4 设 k 是代数封闭域. V 和 W 分别是 k^n 和 k^m 中的代数集合,以 $\mathscr{P}$ 表示从 V 到 W 的多项式映射全体. 以 $\mathscr{H}$ 表示由 $k[W]$ 到 $k[V]$ 的 k-代数同态全体. 则映射

$$\mathscr{P}\to\mathscr{H},f\mapsto f^*$$

是满射. 并且, $f:V\to W$ 为代数集合的同构 $\Longleftrightarrow f^*:h[W]\to k[V]$ 为 k-代数同构. ▌

这就把代数集合的同构和分类问题归结为一类特殊的 k 上的交换代数(有限生成并且没有非零的幂零元素)的同构和分类这一纯代数问题. 让我们举一些例子.

例 4 设 V 为仿射直线, $V=k$. W 是由方程 $x^3=y^2$ 的解给出的不可约平面代数曲线($\subseteq k^2$). 则

$$f:V\to W,t\mapsto(t^2,t^3)\quad(t\in k)$$

是从 V 到 W 的多项式映射,这是因为对每个 $t\in k$, $(t^2,t^3)\in W$ ($(x,y)=(t^2,t^3)$ 满足方程 $x^3=y^2$). 但是它们的坐标环 $k[V]=k[t]$ 和 $k[W]=k[x,y]/(y^2-x^3)=k[x,x^{3/2}]$ 作为 k-代数是不同构的($k[t]$ 为主理想整环,而 $k[x,x^{3/2}]$ 中理想 $(x,x^{3/2})$ 不是主理想). 因此 V 和 W 不同构.

例 5 由 $y=x^n$(n 为正整数)定义的仿射空间 k^2 中平面代数曲线 V 和仿射直线 k 同构. 因为

$$f:V\to k,(x,y)\mapsto x,\qquad g:k\to V,t\mapsto(t,t^n)$$

是互逆的多项式映射.

例 6 设 k 是特征 p 的代数封闭域(p 为素数). 熟知对于每个 $n\geqslant1,q=p^n$, k 中有唯一的一个 q 元子域 $\mathbf{F}_q$. $\mathbf{F}_q$ 即是由方程 $x^q-x=0$ 在 k 中的 q 个不同根组成的. 设 $f_i(x_1,\cdots,x_n)\in\mathbf{F}_q[x_1,\cdots,x_n]$ $(1\leqslant i\leqslant m)$. 而 V 是由方程组

$$f_i(x_1,\cdots,x_n)=0\quad(1\leqslant i\leqslant m)\tag{1}$$

在 k^n 中决定的代数集合. 考虑映射

$$\varphi_l: V\to V, \varphi_l(a_1,\cdots,a_n)=(a_1^{q^l},\cdots,a_n^{q^l}).$$

由于 f_i 的系数属于 $\mathbf{F}_q$，从而若 $f_i(a_1,\cdots,a_n)=0$，则 $f_i(a_1^{q^l},\cdots,a_n^{q^l})=f_i(a_1,\cdots,a_n)^{q^l}=0$. 即若 $(a_1,\cdots,a_n)\in V$，则 $(a_1^{q^l},\cdots,a_n^{q^l})\in V$. 于是 φ_l 是从 V 到 V 自身的多项式映射. 并且：

$(a_1,\cdots,a_n)$ 为方程组(1)在域 $\mathbf{F}_{q^l}$ 中的解

$\Longleftrightarrow(a_1,\cdots,a_n)\in V, a_i\in\mathbf{F}_{q^l}(1\leqslant i\leqslant n)$

$\Longleftrightarrow(a_1,\cdots,a_n)\in V, a_i^{q^l}=a_i(1\leqslant i\leqslant n)$

$\Longleftrightarrow(a_1,\cdots,a_n)\in V, \varphi_l(a_1,\cdots,a_n)=(a_1,\cdots,a_n)$.

$\Longleftrightarrow(a_1,\cdots,a_n)$ 为多项式映射 φ_l 的不动点.

于是，对每个正整数 l，方程组(1) 在 $\mathbf{F}_q$ 的 l 次扩域 $\mathbf{F}_{q^l}$ 中解的个数等于多项式映射 φ_l 的不动点个数. 在代数几何中，φ_l 叫作是 Frobenius 映射. 它在代数几何的算术理论中起着重要的作用.

定义 设 V 和 W 分别是 k^n 和 k^m 中的代数簇. 映射

$$f=(f_1,\cdots,f_m):V\to W$$

叫作从 V 到 W 的**有理映射**，是指

(1) $f_i(x_1,\cdots,x_n)\in k(V)$. $(1\leqslant i\leqslant m)$;

(2) 如果 $f_i(x_1,\cdots,x_n)(1\leqslant i\leqslant m)$ 在点 $(a_1,\cdots,a_n)\in V$ 均有定义时，则 $f(a_1,\cdots,a_n)=(f_1(a_1,\cdots,a_n),\cdots,f_m(a_1,\cdots,a_n))\in W$.

由定义立刻得出：

(A) $f=(f_1,\cdots,f_m):V\to k^m$ 是有理映射 $\Longleftrightarrow f_i\in k(V)$.

(因为 k^m 对应的根式理想为(0). 从而上面条件(2)自然成立.)

(B) 如果又有有理映射 $g:W\to U$ (U 是 k^t 中的代数簇，则 $g\circ f:V\to U$ 也是有理映射(因为有理函数的复合函数仍是有理函数，并且 $g\circ f(V)\subseteq g(W)\subseteq U$).

(C) 多项式映射均是有理映射. 特别地，恒等映射 $1_V:V\to V$ 为有理映射.

定义 设V和W分别是k^n和k^m中的代数簇. 如果存在着有理映射$f:V\to W$和$g:W\to V$,并且对于每个点$P\in V$,当$f(P)$和$g\circ f(P)$均有意义时,则$g\circ f(P)=P$. 同时对于每个点$Q\in W$,当$f\circ g(Q)$有意义时,$f\circ g(Q)=Q$. 则称f和g是**互逆**的有理映射,并且称代数簇V和W是**双有理同构**的.

设$f=(f_1,\cdots,f_m):V\to W$是代数簇之间的有理映射. 对于每个$g(y_1,\cdots,y_m)\in k(W)$,$g:W\to k$是有理映射(见(A)中所述). 从而$g\circ f:V\to k$为有理映射(见(B)中所述),即$g\circ f\in k(V)$. 于是我们由有理映射$f$诱导出:

$$f^*:k(W)\to k(V),\quad g\mapsto f^*(g)=g\circ f.$$

如果W和V均非空,则域$k(W)$和$k(V)$均包含k作为子域. 不难看出f^*是域的k-同态(k-同态即指f^*在k上的限制是恒等映射).

下一定理与定理4是很相似的,但是证明需要更多的代数几何知识.(其麻烦主要在于:一个有理映射$f:V\to W$不是在V的所有点均有定义). 我们略去证明.

定理 5 设k是代数封闭域,V和W分别为k^n和k^m中的代数簇.

(1) 如果$f:V\to W$为有理映射,则$f^*:k(W)\to k(V)$为域的k-同态. 并且对于每个域的k-同态$\varphi:k(W)\to k(V)$,均存在有理映射$f:V\to W$,使得$\varphi=f^*$.

(2) $f:V\to W$为双有理同构$\Longleftrightarrow f^*:k(W)\to k(V)$为域的$k$-同构. ▌

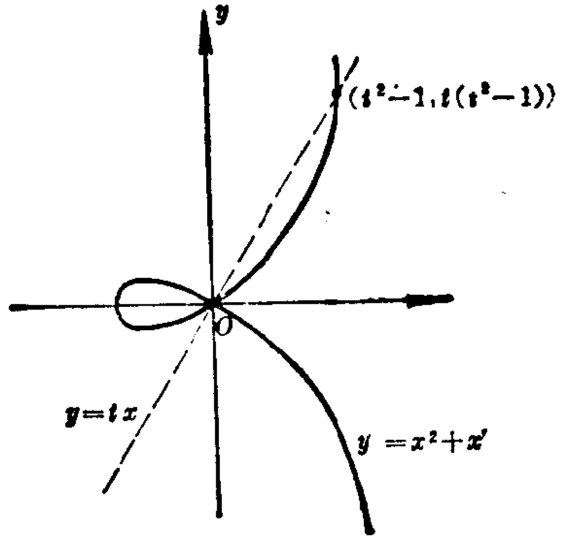
这个定理又把代数簇的双有理同构问题归结为它们的有理函数域是否k-同构这一代数问题.

例 7 设k为代数闭域. 则平面代数曲线$C:y^2=x^2+x^3$是不可约的,因为$y^2-x^2-x^3$是$k[x,y]$中的不可约多项式. 我们

证明它与仿射直线 k 双有理同构. 办法是：斜率为 t 的直线 $y=tx$ 与曲线 C 交于一点：

$$x=t^2-1,\ y=t(t^2-1)$$

(参见示意图). 于是得到有理映射



$$f:k\to C,\ f(t)=(t^2-1,t(t^2-1)).$$

它的逆为有理映射：

$$g:C\to k,\ g(x,y)=y/x.$$

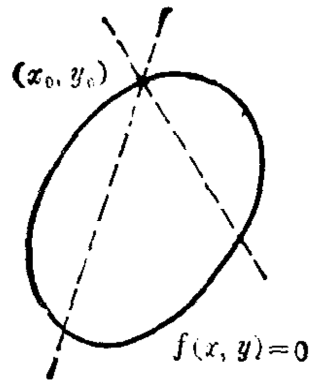
从而 C 与 k 双有理同构，但是它们不同构. 因为 $k[C]=k[x,y]/(y^2-x^2-x^3)\cong k[x,\ x\sqrt{1+x}]$作为环与 $k[\ t\ ]$不同构.

定义 与仿射空间 k^n(对某个 $n\geqslant 1$) 双有理同构的代数簇叫作是**有理代数簇**. 当 $n=1$ 时叫作是有理曲线.

于是例 7 表明 $y^2=x^2+x^3$ 为有理曲线. 有理曲线的进一步的例子为：

例 8 不可约平面二次曲线 $C:f(x,y)=0$ 均是有理曲线，其中 $f(x,y)=ax^2+bxy+cy^2+dx+ey+f$ 是 $k[x,y]$ 中不可约二次多项式.

为了看出曲线 C 的有理性，我们任取 C 上一点(x_0,y_0) (我们



在 § 6.1 证明了，对于代数封闭域 k，每个不可约平面代数曲线均有无穷多个点）。过 (x_0, y_0) 而斜率为 t 的直线 $y-y_0=t(x-x_0)$ 与曲线 C 的交点之 x-坐标满足关于 x 的二次方程 $f(x, y_0+t(x-x_0))=0$（参见示意图）。此式左边设为 $A(t)x^2+B(t)x+C(t)$，它的一个根为 x_0，从而另一个根为 $p(t)=-x_0-\dfrac{B(t)}{A(t)}$，这是 t 的有理函数。于是我们得到有理映射

$$f: k \to C, \quad f(t)=(p(t),\ y_0+t(p(t)-x_0)).$$

它的逆为有理映射

$$g: C \to k, \quad g(x, y)=\frac{y-y_0}{x-x_0}.$$

从而不可约平面二次曲线均为有理曲线。

例 9 现在给出非有理曲线的例子：设 $m \geqslant 3$，代数封闭域 k 的特征为 0，或者特征为素数 π 但是 $\pi \nmid n$。则曲线 $\mathscr{F}: x^n+y^n=1$ 不是有理的。

证明 如果 $\mathscr{F}$ 是有理曲线，则有有理映射

$$f: k \to \mathscr{F}, \quad f(t)=(\varphi(t),\ \psi(t)),$$

其中 $\varphi(t), \psi(t) \in k(t)$，并且 $\varphi(t)^n+\psi(t)^n=1$。令 $\varphi(t)=\dfrac{p(t)}{r(t)}$，

$\psi(t)=\dfrac{q(t)}{r(t)}, p(t), q(t), r(t)\in k[t]$，则

$$p(t)^n+q(t)^n-r(t)^n=0.$$

三个多项式 p,q,r 中任意两个的公因子也必是第三个多项式的因子．将它们的公因子去掉后仍满足上面等式．从而我们可以一开始就假定 p,q,r 两两互素．将上面等式对 t 微商．由于对域 k 特征的假设可知微商后为

$$p^{n-1}p'+q^{n-1}q'-r^{n-1}r'=0.$$

这两个等式可合写成

$$\begin{pmatrix} p & q & r \\ p' & q' & r' \end{pmatrix}\begin{pmatrix} p^{n-1} \\ q^{n-1} \\ -r^{n-1} \end{pmatrix}=\begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

于是

$$p^{n-1}:q^{n-1}:\ (-r^{n-1})=(qr'-q'r):\ (rp'-r'p):\ (pq'-p'q).$$

由于 p,q,r 两两互素，可知 $p^{n-1}|(qr'-rq')$，$q^{n-1}|(rp'-pr')$，$r^{n-1}|(pq'-qp')$．令 $\deg p=a, \deg q=b, \deg r=c$．不妨设 $a\geqslant b\geqslant c$．则由 $p^{n-1}|(qr'-rq')$ 可知 $(n-1)a\leqslant b+c-1$．但在 $a\geqslant b\geqslant c$ 和 $n\geqslant 3$ 的时候，$(n-1)a\geqslant 2a\geqslant b+c>b+c-1$．由此导出矛盾．从而曲线 $\mathscr{F}$ 不是有理的．

研究代数簇的双有理同构分类和双有理不变量是代数几何的核心问题之一．若代数簇 V 和 W 双有理同构，则它们的有理函数域 $k(V)$ 和 $k(W)$ 是 k-同构的．特别地，它们在 k 上的超越次数相同．我们把 $k(V)$ 在 k 上的超越次数称作是代数簇 V 的**维数**．于是，双有理同构的代数簇有相同的维数，即维数是双有理不变量．维数的这个代数定义方式与几何直观上一个代数簇的维数概念是一致的．

一维代数簇，即不可约代数曲线的另一个重要的双有理不变

量是所谓亏格 g(genus)．限于篇幅，我们不能在这里讲亏格的严格定义．只是想指出，代数封闭域 k 上亏格为 0 的不可约曲线均是有理曲线，即均双有理同构于仿射直线 k．从而亏格为 0 的不可约曲线只有一个双有理同构类．亏格为 1 的不可约代数曲线叫作是**椭圆曲线**．它们可分成无穷多个双有理同构类．事实上，可以构作出一个 k 上的一维代数簇 $\mathscr{M}$，使得 $\mathscr{M}$ 上点一一对应于 k 上的椭圆曲线双有理同构类．一般地，对于某一族具有特定性质的代数簇 $\mathscr{F}$，如果我们能将 $\mathscr{F}$ 中成员的双有理同构类很好地参数化，即如果我们能找到一个 k 上代数簇 $\mathscr{M}$，使得 $\mathscr{F}$ 中每个代数簇双有理同构类一一对应于 $\mathscr{M}$ 中点，则称 $\mathscr{M}$ 为 $\mathscr{F}$ 的 moduli．于是 k 上椭圆曲线族的 moduli 是 k 上一个一维代数簇．而当 $g \geqslant 2$ 时，亏格为 g 的不可约代数曲线族的 moduli 是一个 $3g-3$ 维的代数簇．寻求和构作某一类代数簇之 moduli，也是代数几何一个基本问题．上世纪由 Riemann 等人对于复数域 C 上的代数曲线作了这方面的开创性工作．本世纪六十年代美国数学家 Mumford 在 moduli 问题上作了出色的工作，获得 1970 年 Fields 奖．

Euler 在研究不定积分运算的过程中最早考虑到曲线之间的双有理同构性质．设 $f(x,y)=0$ 为复数域 C 上一条不可约平面代数曲线，则 y 为 x 的函数：$y=y(x)$．对于每个有理函数 $F(X,Y)\in \mathbf{C}[X,Y]$，研究不定积分

$$I=\int F(x,y(x))dx$$

的计算问题．一个重要问题是：这个不定积分是否可以表达成初等函数形式？当曲线 $C: f(x,y)=0$ 为有理曲线时，答案是肯定的．因为设 $\varphi: k\to C$，$\psi: C\to k$ 为互逆的有理映射，$\varphi(t)=(\varphi_1(t),\varphi_2(t))$，则 $\varphi_1(t)$，$\varphi_2(t)\in k(t)$，$\psi(x, y)\in k(x, y)$，于是 $I=\int F(\varphi_1(t),\varphi_2(t))\varphi_1'(t)dt$．此时被积函数是 t 的有理函数．

从而 I 是 t 的初等函数. 再代入 $t=\psi(x,y)$，即将 I 表成 x 和 y 的初等函数形式.

比如说，根据例 8，每个复数域 C 上的不可约二次曲线 $C:y^2=ax^2+bx+c$ 均是有理曲线（a，b，$c\in C$）. 从而不定积分 $I=\int F(x,\sqrt{ax^2+bx+c})dx$ 均可表成 x 和 $\sqrt{ax^2+bx+c}$ 的初等函数，从而也是 x 的初等函数. 而例 8 中给出的曲线 C 与仿射直线 k 之间互逆的有理映射，就是计算不定积分 I 时所采用的 Euler 变量代换.

又如：当 $e\neq1$ 时，曲线 $C:y^2=(1-x^2)(1-ex^2)$ 的亏格为 1，即为椭圆曲线而不是有理曲线. 不定积分

$$I_0=\int\frac{dx}{\sqrt{(1-x^2)(1-ex^2)}}$$

不能表成 x 的初等函数. I_0 是椭圆积分，而它定义出的函数叫椭圆函数.

最后我们谈谈交换代数中的局部化方法在研究代数簇局部性质和整体性质的过程中所起的作用. 设 k 为代数封闭域，V 为 k^n 中的代数集合. 对于 V 上每个点 $P=(a_1,\cdots,a_n)$，$\mathrm{m}_P=\{f(x_1,\cdots,x_n)\in k[V]\mid f(a_1,\cdots,a_n)=0\}$ 是坐标环 $k[V]$ 的极大理想，并且每个极大理想均有如此的形式. 我们把局部环 $k[V]_{\mathrm{m}_P}$ 叫作是**代数集合 V 在点 P 处的局部环**. 如果 V 为代数簇，则 $k[V]$ 是整环，$k[V]$ 可看作是 $k[V]_{\mathrm{m}_P}$ 的子环，而 $k[V]$ 和 $k[V]_{\mathrm{m}_P}$ 的商域均是 V 的有理函数域 $k(V)$，并且

$$k[V]_{\mathrm{m}_P}=\left\{\frac{f(x_1,\cdots,x_n)}{g(x_1,\cdots,x_n)}\middle| f,g\in k[V],g(a_1,\cdots,a_n)\neq0\right\}$$

$$=\{f/g\in k(V)\mid f,g\in k[V],f/g\text{ 在}(a_1,\cdots,a_n)\text{有定义}\}.$$

在点 $P=(a_1,\cdots,a_n)\in V$ 处有定义的有理函数叫作是在点 P **正**

则的函数. 于是局部环 $k[V]_{\mathfrak{m}_P}$ 即是在点 P 处正则的有理函数环. 这是 Noether 局部整环. 我们知道，对于任意整环 R，均有 $R=\bigcap_{\mathfrak{p}\in\operatorname{Spec}R}R_{\mathfrak{p}}=\bigcap_{\mathfrak{m}\in\operatorname{Max}R}R_{\mathfrak{m}}$（§3.2 习题 3）. 取 $R=k[V]$，我们便有

$$k[V]=\bigcap_{P\in V}k[V]_{\mathfrak{m}_P}.$$

它的几何意义即是：代数簇 V 上的一个有理函数如果在 V 的每点均正则，则必为多项式函数.

利用局部环 $k[V]_{\mathfrak{m}_P}$ 我们还可研究代数簇 V 在点 P 的奇异特性，以及两个代数簇在公共点 P 处的相交特性等. 还可以通过局部来把握 V 的整体特性. 我们这里就不仔细讲述了.

习　题

（k 均为代数封闭域）

1. 设 X 和 Y 为 k^n 和 k^m 中的代数集合. 求证有 k-代数同构：$k[X\times Y]\cong k[X]\otimes_k k[Y]$（右边为 k-代数的张量积，参见 §6.2 习题 5）.

2. k^2 中曲线 $x^3=y^2$ 与仿射直线 k 双有理同构但是不同构. 试给出曲线 $x^3=y^2$ 与仿射直线之间一对互逆的有理映射.

3. 设 V 是 k^3 中由 $y^2=xz$ 和 $z^2=y^3$ 定义的代数集合. 试将 V 分解成有限个互不包含的代数簇之并. 并证明每个代数簇分支均双有理同构于仿射直线.

4. (1) 证明 $\{(t,t^2,t^3)\in k^3\mid t\in k\}$ 是有理曲线.

(2) 证明 $(x^2+y^2)^2=a^2(x^2-y^2)$ $(a\in k)$ 为 k^2 中有理曲线. [提示：研究此曲线与 $x^2+y^2=t(x-y)$ 的交点.]

(3) 求证极坐标表示的平面 k^2 中代数曲线 $r=\sin 3\varphi$ 为有理曲线.

(4) 求证 k^2 中双曲线 $xy=1$ 与仿射直线 k 双有理同构但是不同构.

§ 6.4 代数整数环

现在谈代数数论. 我们在第五章§5.3中证明了，每个代数数域K(即有理数域Q的有限次扩张)的代数整数环O_K(即Z在K中的整闭包)均是Dedekind整环、从而O_K的非零分式理想全体形成群，今后这个群表示成$I(K)$，这是以O_K中全部非零素理想为基的自由Abel群. 另一方面，O_K的主分式理想全体形成$I(K)$的子群，今后记成$P(K)$. 可以证明，O_K的理想类群(或叫作是K的理想类群)$C(K)=I(K)/P(K)$是有限Abel群. 我们在第五章末尾还证明了：O_K(或K)的理想类数$h(K)=|C(K)|$为$1 \Longleftrightarrow O_K$是唯一因子分解整环$\Longleftrightarrow O_K$为主理想整环. 如果考虑乘法群$K^*=K-\{0\}$到群$P(K)$的同态：$\alpha \to (\alpha)=\alpha O_K$，易知这是满同态并且核为$O_K$的单位群$U(O_K)$，这个单位群今后记为$U(K)$. 在代数数论中对于$U(K)$的结构也有很明确的结果. 于是，代数数论最基本的研究对象体现在下面两个Abel群正合序列之中：

$$1 \to P(K) \to I(K) \to C(K) \to 1,$$
$$1 \to U(K) \to K^* \to P(K) \to 1.$$

自然会提出如下一些问题：

问题 1 对于给定的代数数域K，如何决定它的代数整数环O_K?

问题 2 每个素数p在Dedekind整环O_K中的扩张理想pO_K应当有素理想因子分解式：$pO_K=\mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_g^{e_g}$，如何决定这个分解式?

问题 3 如何计算O_K的理想类数$h(K)$?

……

在这一节中，对于任意代数整数环O_K，我们就前两个问题给出某些一般性结果. 在下一节中，我们对一类特殊的代数数域——

二次域给出更具体的答案和某些应用.

关于问题1，首先有如下的一般性结果.

定理 6 设K为n次代数数域(即$[K:\mathbf{Q}]=\dim_{\mathbf{Q}}K=n$)，则代数整数环$O_K$是秩为$n$的自由$\mathbf{Z}$-模.

证明 设$\alpha_1,\cdots,\alpha_n$为$\mathbf{Q}$上n维向量空间K的一组基.必要时乘以一个大的自然数，我们不妨设$\alpha_i\in O_K(1\leqslant i\leqslant n)$. 我们在§5.3定理7的证明中知道存在非零有理整数d，使得O_K是自由$\mathbf{Z}$-模$\frac{\alpha_1}{d}\mathbf{Z}\oplus\cdots\oplus\frac{\alpha_n}{d}\mathbf{Z}$的$\mathbf{Z}$-子模. 但是自由$\mathbf{Z}$-模的子模仍是自由$\mathbf{Z}$-模，从而$O_K$为自由$\mathbf{Z}$-模，并且$\mathrm{rank}_{\mathbf{Z}}O_K\leqslant n$. 由于$\alpha_1,\cdots,\alpha_n$是$O_K$中一组$\mathbf{Q}$-线性无关元素,从而它们也是$\mathbf{Z}$-线性无关的. 由于$\mathrm{rank}_{\mathbf{Z}}O_K$等于$O_K$中$\mathbf{Z}$-线性无关元素的最多个数. 于是$\mathrm{rank}_{\mathbf{Z}}O_K\geqslant n$. 从而$\mathrm{rank}_{\mathbf{Z}}O_K=n$, 即$O_K$是秩$n$的自由$\mathbf{Z}$-模.▌

定义 秩n自由$\mathbf{Z}$-模O_K的每一组基$\omega_1,\cdots,\omega_n$均叫作是O_K(或域K)的一组**整基**.

于是,若$\omega_1,\cdots,\omega_n$为O_K的一组整基,则$O_K=\omega_1\mathbf{Z}\oplus\cdots\oplus\omega_n\mathbf{Z}$. 换句话说,域$K$中每个代数整数(即$O_K$中每个元素)均可唯一的表示成$\alpha=m_1\omega_1+\cdots+m_n\omega_n, m_i\in\mathbf{Z}$. 决定$O_K$的整基是代数数论的很基本问题.

正如向量空间的基有不同取法一样，O_K的整基也可有不同取法. 但是O_K的两组不同的整基有一定的联系. 设$\{\omega_1,\cdots,\omega_n\}$和$\{\omega_1',\cdots,\omega_n'\}$是$O_K$的两组整基,则每个$\omega_i$可表成$\omega_1',\cdots\omega_n'$的$\mathbf{Z}$-线性组合,且反之亦然.于是我们有

$$M\begin{pmatrix}\omega_1'\\ \vdots\\ \omega_n'\end{pmatrix}=\begin{pmatrix}\omega_1\\ \vdots\\ \omega_n\end{pmatrix},\quad N\begin{pmatrix}\omega_1\\ \vdots\\ \omega_n\end{pmatrix}=\begin{pmatrix}\omega_1'\\ \vdots\\ \omega_n'\end{pmatrix},\tag{1}$$

其中M和N为n阶方阵并且元素属于$\mathbf{Z}$. 由于$\{\omega_i\}$和$\{\omega_i'\}$均为整基,可知$MN=I_n$(n阶单位矩阵). 从而$\det M\cdot\det N=1$. 但是$\det M\in\mathbf{Z}$. 于是$\det M=\pm1$.反之,如果$\{\omega_i'\}$是一组整基,M是元素属于$\mathbf{Z}$的n阶方阵,并且$\det M=\pm1$,则M是可逆方阵,并且逆M^{-1}的元素也属于$\mathbf{Z}$. 从而由(1)式第一式定义的$\{\omega_i\}$必然也是整基. 这就证明了:O_K的不同整基之间的变换方阵是元素属于$\mathbf{Z}$且行列式为±1的n阶方阵.

设$\sigma_1,\cdots,\sigma_n$是代数数域K到复数域$\mathbf{C}$中的n个不同的嵌入(见§5.3定理7的证明所述,注意$K/\mathbf{Q}$必然是域的可分扩张,从而嵌入个数等于$n=[K:\mathbf{Q}]$),不妨设σ_1为恒等嵌入. 由于每个σ_i在$\mathbf{Q}$上的限制都是恒等映射(因为$\mathbf{Q}$只有唯一的自同构),从而由(1)式得到

$$\begin{pmatrix}\sigma_1(\omega_1)\cdots\sigma_n(\omega_1)\\ \cdots\\ \sigma_1(\omega_n)\cdots\sigma_n(\omega_n)\end{pmatrix}=M\begin{pmatrix}\sigma_1(\omega_1')\cdots\sigma_n(\omega_1')\\ \cdots\\ \sigma_1(\omega_n')\cdots\sigma_n(\omega_n')\end{pmatrix}.$$

于是

$$(T(\omega_i\omega_j))=M(T(\omega_i'\omega_j'))M^T, \tag{2}$$

其中$T(\alpha)=\sum_{i=1}^{n}\sigma_i(\alpha)(\alpha\in K)$即是§5.3定理7 证明中定义的元素$\alpha$的迹,$T(\alpha)\in\mathbf{Q}$. 并且当$\alpha\in O_K$时,那里证明了$T(\alpha)\in\mathbf{Z}$.

定义 设$\alpha_1,\cdots,\alpha_n\in K$,则$\mathbf{Q}$中元素
$\Delta(\alpha_1,\cdots,\alpha_n)=\det(T(\alpha_i\alpha_j))_{1\leqslant i,j\leqslant n}=$

$$\begin{vmatrix}\sigma_1(\alpha_1)\cdots\sigma_n(\alpha_1)\\ \cdots\quad\cdots\\ \sigma_1(\alpha_n)\cdots\sigma_n(\alpha_n)\end{vmatrix}\begin{vmatrix}\sigma_1(\alpha_1)\cdots\sigma_1(\alpha_n)\\ \cdots\\ \sigma_n(\alpha_1)\cdots\sigma_n(\alpha_n)\end{vmatrix}$$

为$\{\alpha_1,\cdots,\alpha_n\}$的判别式．如果$\alpha_i\in O_K(1\leqslant i\leqslant n)$，则$\Delta(\alpha_1,\cdots,\alpha_n)\in\mathbf{Z}$.

下一引理表明判别式可用来判别$\{\alpha_1,\cdots,\alpha_n\}$是否可作为$\mathbf{Q}$-向量空间$K$的一组基.

引理 3 设K为n次代数数域，$\alpha_1,\cdots,\alpha_n\in K$，则

(1) $\Delta(\alpha_1,\cdots,\alpha_n)\neq 0\Longleftrightarrow\alpha_1,\cdots,\alpha_n$是$\mathbf{Q}$-线性无关的.

(2) 如果$\{\omega_1,\cdots,\omega_n\}$是$O_K$的一组整基，则$\Delta(\omega_1,\cdots,\omega_n)$由$O_K$所决定而与整基$\{\omega_i\}$的选取无关.

证明 (1) 我们知道代数数域K是$\mathbf{Q}$的可分扩张，从而为单扩张．即存在$\alpha\in K$(甚至可取$\alpha\in O_K$)，使得$K=\mathbf{Q}(\alpha)$．于是$1,\alpha,\cdots,\alpha^{n-1}$是$\mathbf{Q}$-向量空间$K$的一组基．而

$$\Delta(1,\alpha,\cdots,\alpha^{n-1})=\begin{vmatrix}1&\cdots&1\\\sigma_1(\alpha)&&\sigma_n(\alpha)\\\vdots&&\vdots\\\sigma_1(\alpha)^{n-1}&\cdots&\sigma_n(\alpha)^{n-1}\end{vmatrix}^2.$$

由于对于域K的生成元α，$\sigma_1(\alpha),\cdots,\sigma_n(\alpha)$是彼此不同的．从而上式右边的Vandemond行列式不为零．于是$\Delta(1,\alpha,\cdots,\alpha^{n-1})\neq 0$.现在对于$K$的任意一组$\mathbf{Q}$-基$\{\alpha_1,\cdots,\alpha_n\}$，则它与基$\{1,\alpha,\cdots,\alpha^{n-1}\}$之间的变换方阵是元素属于$\mathbf{Q}$的$n$阶非异方阵$M$．于是$\Delta(\alpha_1,\cdots,\alpha_n)$和$\Delta(1,\alpha,\cdots,\alpha^{n-1})$相差因子$(\det(M))^2\neq 0$．即$\Delta(\alpha_1,\cdots,\alpha_n)\neq 0$．反之，如果$\alpha_1,\cdots,\alpha_n$不是$K$的一组$\mathbf{Q}$-基，即它们是$\mathbf{Q}$-线性相关的．则

$$\begin{pmatrix}\alpha_1\\\vdots\\\alpha_n\end{pmatrix}=M\begin{pmatrix}1\\\alpha\\\vdots\\\alpha^{n-1}\end{pmatrix}.$$

其中$\det(M)=0$．从而$\Delta(\alpha_1,\cdots,\alpha_n)=(\det(M))^2\cdot\Delta(1,\alpha,\cdots,\alpha^{n-1})=0$.

(2) 设$\{\omega_1,\cdots,\omega_n\}$和$\{\omega_1',\cdots,\omega_n'\}$是$O_K$的两组整基. 则它们的变换方阵$M$的元素属于$\mathbf{Z}$,并且行列式为$\pm 1$. 于是$\Delta(\omega_1,\cdots,\omega_n)$和$\Delta(\omega_1',\cdots,\omega_n')$相差因子$(\det(M))^2=1$.即$\Delta(\omega_1,\cdots,\omega_n)=\Delta(\omega_1',\cdots,\omega_n')$. 这就表明$\Delta(\omega_1,\cdots,\omega_n)$是$O_K$(或$K$)本身的特性,与整基的选取方法无关.▌

定义 $\Delta(\omega_1,\cdots,\omega_n)$叫作是$\mathbf{Q}_K$(或域$K$)的判别式,表示成$d(K)$. 由于整基$\{\omega_1,\cdots,\omega_n\}$必然也是域$K$的$\mathbf{Q}$-基,从而$d(K)$是非零的有理整数.

判别式$d(K)$对于寻求O_K的整基是有益处的.

引理 4 设K为n次代数数域,$d(K)$是K的判别式.$\alpha_1,\cdots,\alpha_n\in O_K$并且$\Delta(\alpha_1,\cdots,\alpha_n)\neq 0$. 则

(1) $\alpha_1,\cdots,\alpha_n$是O_K的一组整基$\Longleftrightarrow\Delta(\alpha_1,\cdots,\alpha_n)=d(K)$.

(2) 如果有理整数$\Delta(\alpha_1,\cdots,\alpha_n)$没有平方因子(即不被大于1的某个自然数的平方所整除),则$\alpha_1,\cdots,\alpha_n$为O_K的整基.

证明 (1) $\Rightarrow$根据定义.

$\Leftarrow$: 由于$\alpha_1,\cdots,\alpha_n\in O_K$,从而有元素属于$\mathbf{Z}$的$n$阶方阵$M$使得

$$\begin{pmatrix}\alpha_1\\ \vdots\\ \alpha_n\end{pmatrix}=M\begin{pmatrix}\omega_1\\ \vdots\\ \omega_n\end{pmatrix}.$$

其中$\{\omega_1,\cdots,\omega_n\}$是$O_K$的任意一组整基. 于是$\Delta(\alpha_1,\cdots,\alpha_n)=(\det(M))^2\cdot d(K)$. 从而

$\Delta(\alpha_1,\cdots,\alpha_n)=d(K)\Longleftrightarrow\det(M)=\pm 1\Longleftrightarrow\alpha_1,\cdots,\alpha_n$为$O_K$的一组整基.

(2) 如果$\alpha_1,\cdots,\alpha_n$不为整基,则对于上面的方阵M我们有$|\det(M)|\geqslant 2$. 从而$(\det(M))^2|\Delta(\alpha_1,\cdots,\alpha_n)\in\mathbf{Z}$. 这与假定

$\Delta(\alpha_1,\cdots,\alpha_n)$无平方因子相矛盾. 从而 $\alpha_1,\cdots,\alpha_n$ 必然是 O_K 的一组整基. ▌

例 1 设 $K=\mathbf{B}(\sqrt{-19})$,这是二次域. 注意$\frac{1}{2}\left(1+\sqrt{-19}\right)\in O_K$,因为它是首一多项式 $x^2-x+5\in\mathbf{Z}[x]$ 的根. K 在 $\mathbf{C}$ 中的两个嵌入是恒等映射和共轭映射 σ,其中 $\sigma(a+b\sqrt{-19})=a-b\sqrt{-19}(a,b\in\mathbf{Q})$. 从而 1 和$\frac{1}{2}\left(1+\sqrt{-19}\right)$的判别式为

$$\Delta\left(1,\frac{1}{2}\left(1+\sqrt{-19}\right)\right)=\begin{vmatrix}1 & \frac{1}{2}\left(1+\sqrt{-19}\right)\\ 1 & \frac{1}{2}\left(1-\sqrt{-19}\right)\end{vmatrix}^2=-19.$$

由于-19 无平方因子,根据引理 4 可知$\left\{1,\frac{1}{2}\left(1+\sqrt{-19}\right)\right\}$是 O_K 的一组整基. 于是 $O_K=\mathbf{Z}\oplus\mathbf{Z}\left(\frac{1}{2}+\frac{1}{2}\sqrt{-19}\right)=\mathbf{Z}\left[\frac{1}{2}+\frac{1}{2}\sqrt{-19}\right]$. 并且 $d(K)=-19$.

例 2 x^5-x+1 是 $\mathbf{Q}[x]$中不可约多项式(由于 x^5-x+1 (mod 5)不可约,从而在 $\mathbf{Z}[x]$ 中不可约,于是在 $\mathbf{Q}[x]$ 中也不可约). 令 θ 是此多项式在 $\mathbf{C}$ 中的一个根. 则 $K=\mathbf{Q}(\theta)$ 为五次域,并且 $\theta\in O_K$. 设 θ 的共轭元素为 $\theta_1=\theta,\theta_2,\cdots,\theta_5$. 则

$$\Delta(1,\theta,\theta^2,\theta^3,\theta^4)=\det(T(\theta^{i+j}))_{0<i,j<4}$$

$$=\begin{vmatrix}5 & s_1 & s_2 & s_3 & s_4\\ s_1 & s_2 & s_3 & s_4 & s_5\\ s_2 & s_3 & s_4 & s_5 & s_6\\ s_3 & s_4 & s_5 & s_6 & s_7\\ s_4 & s_5 & s_6 & s_7 & s_8\end{vmatrix}$$

其中 $s_i=T(\theta^i)=\sum_{k=1}^{5}\theta_k^i$，这是 $\theta_1,\cdots,\theta_5$ 的对称函数，从而可以表成 $\theta_1,\cdots,\theta_5$ 的初等对称函数（即 x^5-x+1 的诸系数）的多项式，由此可算出 $\Delta(1,\theta,\theta^2,\theta^3,\theta^4)=19\times151$. 它没有平方因子. 于是 $\{1,\theta,\theta^2,\theta^3,\theta^4\}$ 是 O_K 的整基，即 $O_K=\mathbf{Z}[\theta]$，而 $d(K)=19\times151$.（习题中给出计算 $\Delta(1,\theta,\theta^2,\theta^3,\theta^4)$ 的更好办法）.

我们在§5.3定理7的证明中曾定义元素 $\alpha\in K$ 的范 $N(\alpha)=\prod_{i=1}^{n}\sigma_i(\alpha)\in\mathbf{Q}$. 并且当 $\alpha\in O_K$ 时，$N(\alpha)\in\mathbf{Z}$. 现在我们来定义 O_K 中理想（O_K 中的理想称为**整理想**）的范. 设 $\mathfrak{a}$ 为 O_K 的非零整理想，则 $\mathfrak{a}$ 是 O_K 的一个 $\mathbf{Z}$-子模. 由于 O_K 是秩 n 的自由 $\mathbf{Z}$-模（引理1），从而子模 $\mathfrak{a}$ 也是自由 $\mathbf{Z}$-模，并且 $\operatorname{rank}_{\mathbf{Z}}\mathfrak{a}\leqslant n$. 另一方面，$\mathfrak{a}\cap\mathbf{Z}$ 是 $\mathbf{Z}$ 的非零理想（因为若 $0\neq\alpha\in\mathfrak{a}$，则 $0\neq N(\alpha)\in\mathfrak{a}\cap\mathbf{Z}$）. 从而 $(m)=\mathbf{Z}\cap\mathfrak{a}$，其中 m 为自然数. 于是当 $\{\omega_1,\cdots,\omega_n\}$ 为 O_K 的一组整基时，$m\omega_i\in\mathfrak{a}(1\leqslant i\leqslant n)$. 并且 $\mathfrak{a}$ 中元素 $m\omega_1,\cdots,m\omega_n$ 是 $\mathbf{Z}$-线性无关的、这就表明 $\operatorname{rank}_{\mathbf{Z}}\mathfrak{a}=n$，即 $\mathfrak{a}$ 也是秩 n 的自由 $\mathbf{Z}$-模. 设 $\mathfrak{a}=\alpha_1\mathbf{Z}\oplus\cdots\oplus\alpha_n\mathbf{Z}$. 则

$$\begin{pmatrix}\alpha_1\\ \vdots\\ \alpha_n\end{pmatrix}=A\begin{pmatrix}\omega_1\\ \vdots\\ \omega_n\end{pmatrix},$$

其中 $A=(a_{ij})$ 为 n 阶方阵，$a_{ij}\in\mathbf{Z}$ 并且 $\det(A)\neq0$. 如果 $\{\omega_i'\}$ 是 O_K 的另一组整基，$\mathfrak{a}=\alpha_1'\mathbf{Z}\oplus\cdots\oplus\alpha_n'\mathbf{Z}$，则

$$\begin{pmatrix}\alpha_1'\\ \vdots\\ \alpha_n'\end{pmatrix}=M\begin{pmatrix}\alpha_1\\ \vdots\\ \alpha_n\end{pmatrix},\quad\begin{pmatrix}\omega_1\\ \vdots\\ \omega_n\end{pmatrix}=N\begin{pmatrix}\omega_1'\\ \vdots\\ \omega_n'\end{pmatrix}.$$

其中 M 和 N 均为元素属于 $\mathbf{Z}$ 的 n 阶方阵. 而 $\det(M)=\det(N)=$

± 1. 由于

$$\begin{pmatrix} \alpha_1' \\ \vdots \\ \alpha_n' \end{pmatrix} = MAN \begin{pmatrix} \omega_1' \\ \vdots \\ \omega_n' \end{pmatrix}.$$

从而$|\det(A)| = |\det(MAN)|$，这表明$|\det(A)|$与自由 $\mathbf{Z}$-模 $\mathfrak{a}$ 的基$\{\alpha_i\}$和O_K的整基$\{\omega_i\}$的不同取法无关,即它是理想 $\mathfrak{a}$ 本身的性质.

定义 $|\det(A)|$称作是**非零整理想 $\mathfrak{a}$ 的范**，表示成 $N(\mathfrak{a})$.

由定义易知 $N(O_K)=1$ (取 $\{\alpha_1,\cdots,\alpha_n\}=\{\omega_1,\cdots,\omega_n\}$，可知 $A=I_n$).

理想的范有如下一些基本性质.

引理 5 设K为n次代数数域，$\mathfrak{a}$为O_K中非零整理想. 则

(1) 商环$O_K/\mathfrak{a}$是有限环,并且 $N(\mathfrak{a})=|O_K/\mathfrak{a}|$.

(2) 如果 $\mathfrak{a}=\mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_t^{e_t}$ 是 $\mathfrak{a}$ 的素理想分解式，其中 $\mathfrak{p}_1,\cdots,\mathfrak{p}$ 是O_K中两两不同的素理想，$e_i\geqslant 1$，则 $N(\mathfrak{a})=N(\mathfrak{p}_1)^{\alpha_1}\cdots N(\mathfrak{p}_t)^{\alpha_t}$.

(3) 设 $\mathfrak{b}$ 也是O_K中非零整理想,则 $N(\mathfrak{a}\mathfrak{b})=N(\mathfrak{a})N(\mathfrak{b})$.

(4) 设$\{\alpha_1,\cdots,\alpha_n\}$是 $\mathfrak{a}$ 的一组 $\mathbf{Z}$-基，则 $d(\alpha_1,\cdots,\alpha_n)=N(\mathfrak{a})^2 d(K)$.

(5) 对于 $0\neq\alpha\in O_K$,则 $N(\alpha O_K)=N(\alpha)$ （右边为元素 α 的范).

证明 (1) 根据§2.6. 定理 12, 我们可以取O_K的一组整基 $\omega_1,\cdots,\omega_n$,使得$O_K=\omega_1\mathbf{Z}\oplus\cdots\oplus\omega_n\mathbf{Z}$, $\mathfrak{a}=a_1\omega_1\mathbf{Z}\oplus\cdots\oplus a_n\omega_n\mathbf{Z}$, $a_i\in\mathbf{Z}$. 于是

$$\begin{pmatrix} a_1\omega_1 \\ \vdots \\ a_n\omega_n \end{pmatrix} = \begin{pmatrix} a_1 & & \\ & \ddots & \\ & & a_n \end{pmatrix} \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix}.$$

由定义即知 $N(\mathfrak{a})=|a_1\cdots a_n|$. 另一方面，我们有 Z-模同构

$$\begin{aligned}O_K/\mathfrak{a}&=(\omega_1\mathbf{Z}\oplus\cdots\oplus\omega_n\mathbf{Z})/(a_1\omega_1\mathbf{Z}\oplus\cdots\oplus a_n\omega_n\mathbf{Z})\\&\cong\omega_1\mathbf{Z}/a_1\omega_1\mathbf{Z}\oplus\cdots\oplus\omega_n\mathbf{Z}/a_n\omega_n\mathbf{Z}\cong\mathbf{Z}/a_1\mathbf{Z}\oplus\cdots\oplus\mathbf{Z}/a_n\mathbf{Z}.\end{aligned}$$

于是 $|O_K/\mathfrak{a}|=|a_1\cdots a_n|=N(\mathfrak{a})$.

(2) 由中国剩余定理我们有环的同构：

$$O_K/\mathfrak{a}\cong O_K/\mathfrak{p}_1^{e_1}\oplus\cdots\oplus O_K/\mathfrak{p}_t^{e_t}.$$

因此 $N(\mathfrak{a})=|O_K/\mathfrak{a}|=\prod_{i=1}^{t}|O_K/\mathfrak{p}_i^{e_i}|=\prod_{i=1}^{t}N(\mathfrak{p}_i^{e_i})$. 我们只需再证：对于每个 $(0)\neq\mathfrak{p}\in\operatorname{Spec}O_K$，和 $e\geqslant1$，均有 $N(\mathfrak{p}^e)=N(\mathfrak{p})^e$ 即可. 对每个 $k\geqslant1$，取 $\alpha\in\mathfrak{p}^k-\mathfrak{p}^{k+1}$，并作映射

$$\varphi:O_K\to\frac{\alpha O_K+\mathfrak{p}^{k+1}}{\mathfrak{p}^{k+1}},\ x\mapsto\alpha x\ (\operatorname{mod}\ \mathfrak{p}^{k+1}).$$

由 α 的选取可知 $(\alpha)=\mathfrak{p}^k\cdot\mathfrak{a}'$，其中 $\mathfrak{a}'$ 是与 $\mathfrak{p}$ 互素的整理想. 于是 $\alpha O_K+\mathfrak{p}^{k+1}=((\alpha),\mathfrak{p}^{k+1})=(\mathfrak{p}^k\mathfrak{a}',\mathfrak{p}^{k+1})=\mathfrak{p}^k$. 从而 φ 是从 O_K 到 $\mathfrak{p}_k/\mathfrak{p}_{k+1}$ 的 O_K-模满同态. 另一方面，

$$\begin{aligned}x\in\operatorname{Ker}\varphi&\Longleftrightarrow(\alpha x)\subseteq\mathfrak{p}^{k+1}\Longleftrightarrow\mathfrak{p}^{k+1}\,|\,(\alpha x)=\mathfrak{p}^k\mathfrak{a}'(x)\\&\Longleftrightarrow\mathfrak{p}\,|\,(x)\Longleftrightarrow x\in\mathfrak{p}.\end{aligned}$$

从而 $\operatorname{Ker}\varphi=\mathfrak{p}$. 因此我们有 O_K-模同构 $O^k/\mathfrak{p}\cong\mathfrak{p}^k/\mathfrak{p}^{k+1}$. 于是

$$\begin{aligned}N(\mathfrak{p}^e)&=|O_K/\mathfrak{p}^e|=|O_K/\mathfrak{p}|\cdot|\mathfrak{p}/\mathfrak{p}^2|\cdots|\mathfrak{p}^{e-1}/\mathfrak{p}^e|\\&=|O_K/\mathfrak{p}|^e=N(\mathfrak{p})^e.\end{aligned}$$

(3) 将 $\mathfrak{a}$ 和 $\mathfrak{b}$ 表成素理想分解式之后，由(2)立刻得出(3).

(4) 令

$$\begin{pmatrix}\alpha_1\\\vdots\\\alpha_n\end{pmatrix}=M\begin{pmatrix}\omega_1\\\vdots\\\omega_n\end{pmatrix}$$

由定义知 $N(\mathfrak{a})=|\det(M)|$. 设 $\sigma_1,\cdots,\sigma_n$ 是 K 到 $\mathbf{C}$ 中的 n 个嵌入，则 $(\sigma_i(\alpha_j))=M(\sigma_i(\omega_j))$. 于是

$$\Delta(\alpha_1,\cdots,\alpha_n)=(\det(\sigma_i(\alpha_j)))^2=(\det(M))^2(\det(\sigma_i(\omega_j)))^2$$
$$=N(\mathfrak{a})^2\Delta(\omega_1,\cdots,\omega_n)=N(\mathfrak{a})^2d(K).$$

(5) 若 $\mathfrak{a}=(\alpha)$. 则 $\alpha\omega_1,\cdots,\alpha\omega_n$ 是 $\mathfrak{a}$ 的一组 $\mathbf{Z}$-基. 由(4)知 $\Delta(\alpha\omega_1,\cdots,\alpha\omega_n)=N(\mathfrak{a})^2d(K)$. 但是另一方面,

$$d(\alpha\omega,\cdots,\alpha\omega_n)=(\det(\sigma_i(\alpha)\sigma_i(\omega_j)))^2$$
$$=\left(\prod_{i=1}^{n}\sigma_i(\alpha)\right)^2(\det(\sigma_i(\omega_j)))^2$$
$$=N(\alpha)^2d(K).$$

于是 $|N(\alpha)|=N(\mathfrak{a})$. ▌

现在我们转而研究问题 2. 即对每个素数 p,如何得出 pO_k 在 Dedekind 整环 O_K 中的素理想分解式

$$pO_K=\mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_g^{e_g},\tag{1}$$

其中 $\mathfrak{p}_1,\cdots,\mathfrak{p}_g$ 为 O_K 中两两不同的非零素理想, $e_i\geqslant1(1\leqslant i\leqslant g)$.

由于 $\mathfrak{p}_i$ 在 $\mathbf{Z}$ 中的限制是 $\mathbf{Z}$ 的非零素理想, 但是 $p\in\mathfrak{p}_i$, 从而 $\mathfrak{p}_i\cap\mathbf{Z}=p\mathbf{Z}$. 另方面,对 O_K 的其他非零素理想 $\mathfrak{p}\neq\mathfrak{p}_i(1\leqslant i\leqslant g)$, 则 $\mathfrak{p}$ 与 $pO_K=\mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_g^{e_g}$ 互素. 从而 $\mathfrak{p}\cap\mathbf{Z}\neq p\mathbf{Z}$. 这至少在理论上刻画出 O_K 的哪些素理想 $\mathfrak{p}$ 可作为 pO_K 的素理想因子, 即 $\mathfrak{p}\cap\mathbf{Z}=p\mathbf{Z}$(或者写成 $p\in\mathfrak{p}$)的那些素理想 $\mathfrak{p}$.

作环的同态 $\varphi:\mathbf{Z}\to O_K/\mathfrak{p}_i$, $n\mapsto n(\bmod\ \mathfrak{p}_i)$. $\operatorname{Ker}\varphi=\mathbf{Z}\cap\mathfrak{p}_i=p\mathbf{Z}$. 于是给出环的单同态 $\mathbf{Z}/p\mathbf{Z}\to O_K/\mathfrak{p}_i$. 但是两边均是域, 而且均是有限域. 因此域 $O_K/\mathfrak{p}_i$ 是 p 元域 $\mathbf{Z}/p\mathbf{Z}$ 的有限次扩张. 从而 $N(\mathfrak{p}_i)=|O_K/\mathfrak{p}_i|=p^{f_i}$. 我们称 $f_i=f_i(p/\mathfrak{p}_i)$ 为 $\mathfrak{p}_i$ 对于 p 的**剩余类次数**,而分解式(1)中的 $e_i=e_i(p/\mathfrak{p}_i)$ 叫作是 $\mathfrak{p}_i$ 对于 p 的**分歧指数**. 这些参数之间有一个简单的公式.

引理 6 设 K 为 n 次代数数域,对于素数 p,(1)式为 pO_K 在 O_K 中的素理想分解式. 则

$$\sum_{i=1}^{g} e_i f_i = n.$$

证明 将分解式(1)两边取范，左边为 $N(pO_K)=N(p)=p^n$（引理5的(5)），右边为 $N(\mathfrak{p}_1)^{e_1}\cdots N(\mathfrak{p}_g)^{e_g}=p^{e_1f_1+\cdots e_gf_g}$. 于是 $n=e_1f_1+\cdots+e_gf_g$. ▌

现在我们给出求分解式(1)的一个颇为有效的方法.

定理 7 设 K 为 n 次数域，$K=\mathbf{Q}(\alpha)$，$\alpha\in O_K$. $f(x)=x^n+c_1x^{n-1}+\cdots+c_n\in\mathbf{Z}[x]$ 是 α 在 $\mathbf{Q}$ 上的极小多项式，则

(1) $\mathbf{Z}[\alpha]$ 为 O_K 的子环，并且加法商群 $O_K/\mathbf{Z}[\alpha]$ 是有限群.

(2) 设 p 是素数并且 $p\nmid|O_K/\mathbf{Z}[\alpha]|$，令 $f(x)$ 在主理想整环 $\mathbf{Z}/p\mathbf{Z}[x]$ 中分解成

$$f(x)=f_1(x)^{e_1}\cdots f_g(x)^{e_g}(\bmod p),$$

其中 $f_1(x),\cdots,f_g(x)$ 是 $\mathbf{Z}[x]$ 中首一多项式，并且看作 $\mathbf{Z}/p\mathbf{Z}[x]$ 中元素时是彼此不同的不可约多项式. 则 $\mathfrak{p}_i=(p,f_i(\alpha))(1\leqslant i\leqslant g)$ 是 O_K 中 g 个两两不同的素理想，并且 pO_K 在 O_K 中素理想分解式为 $pO_K=\mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_g^{e_g}$，而且 $f_i(p/\mathfrak{p}_i)=\deg f_i(x)$ $(1\leqslant i\leqslant g)$.

证明 (1) $\mathbf{Z}[\alpha]$ 显然是 O_K 的子环，并且它们均是秩 n 的自由 $\mathbf{Z}$-模，于是有整基 $\{\omega_1,\cdots,\omega_n\}$，使得 $O_K=\mathbf{Z}\omega_1\oplus\cdots\oplus\mathbf{Z}\omega_n$，$\mathbf{Z}[\alpha]=\mathbf{Z}m_1\omega_1\oplus\cdots\oplus\mathbf{Z}m_n\omega_n$，$m_i\in\mathbf{Z}$. 由于 $\mathrm{rank}_{\mathbf{Z}}\mathbf{Z}[\alpha]=n$，从而 $m_1,\cdots,m_n$ 均不为 0. 于是有 Abel 群同构

$$O_K/\mathbf{Z}[\alpha]\cong\mathbf{Z}/m_1\mathbf{Z}\oplus\cdots\oplus\mathbf{Z}/m_n\mathbf{Z},$$

从而 $|O_K/\mathbf{Z}[\alpha]|=|m_1\cdots m_n|$ 有限.

(2) 令 $f_i=\deg f_i(x)(1\leqslant i\leqslant g)$. 我们先依次证明如下三件事.

(A) 对于每个 i，或者 $\mathfrak{p}_i=O_K$ 或者 O_K/p_i 为 p^{f_i} 元域. 这是因为：$f_i(x)(\bmod p)$ 不可约，从而 $F_i=\mathbf{Z}/p\mathbf{Z}[x]/(f_i(x))$ 为域.

我们有环的自然满同态 $\varphi:\mathbf{Z}[x]\to\dfrac{\mathbf{Z}/p\mathbf{Z}[x]}{(f_i(x))}$, $g(x)\to g(x)$ (mod $p, f_i(x)$). Ker $\varphi=(p,f_i(x))$. 从而有环同构 $\dfrac{\mathbf{Z}[x]}{(p,f_i(x))}\cong\dfrac{\mathbf{Z}/p\mathbf{Z}[x]}{(f_i(x))}$. 但是右边为 p^{f_i} 元域，从而左边也是域. 于是 $(p, f_i(x))$ 是 $\mathbf{Z}[x]$ 的极大理想. 再考虑环的同态

$$\pi:\mathbf{Z}[x]\to O_K/\mathfrak{p}_i,\ f(x)\mapsto f(\alpha)(\text{mod }\mathfrak{p}_i).$$

由于 $\mathfrak{p}_i=(p,f_i(\alpha))$，从而 $(p,f_i(x))\subseteq\text{Ker }\pi$. 但是 $(p,f_i(x))$ 是 $\mathbf{Z}[x]$ 的极大理想，从而 Ker $\pi=(p,f_i(x))$ 或者 Ker $\pi=\mathbf{Z}[x]$. 只需再证明 π 是满同态，即得 (A) 中结论(因 Ker π 的上述两种可能分别对应于 $O_K/\mathfrak{p}_i$ 为 p^{f_i} 元域和 $\mathfrak{p}_i=O_K$ 两种情形). 为证 π 是满同态，又只需证明 $\mathfrak{p}_i+\mathbf{Z}[\alpha]=O_K$. 但是 $\mathfrak{p}_i\supseteq pO_K$，从而又只需证 $pO_K+\mathbf{Z}[\alpha]=O_K$ 即可. 这时我们要利用定理假设 $p\nmid|O_K/\mathbf{Z}[\alpha]|$. 由于 $|O_K/pO_K|=p^n$，而 $R=O_K/(\mathbf{Z}(\alpha)+pO_K)$ 是 $O_K/\mathbf{Z}(\alpha)$ 的商群，从而 $|R|$ 除尽 $|O_K/\mathbf{Z}[\alpha]|$. 同样理由 $|R|$ 也应当除尽 $|O_K/pO_K|$. 但是上述表明 $|O_K/\mathbf{Z}[\alpha]$ 和 $|O_K/pO_K|$ 互素，于是 $|R|=1$，即 $\mathbf{Z}[\alpha]+pO_K=O_K$. 这就完全证明了 (A).

(B) $1\leqslant i\neq j\leqslant g$，则 $(\mathfrak{p}_i,\mathfrak{p}_j)=1$(互素). 这是因为：$f_i(x)$ 和 $f_j(x)$ 是 $\mathbf{Z}/p\mathbf{Z}[x]$ 中不同的不可约多项式，从而有 $h(x)$, $k(x)\in\mathbf{Z}/p\mathbf{Z}[x]$，使得 $h(x)f_i(x)+k(x)f_j(x)\equiv1(\text{mod }p)$. 代入 α 得到 $f_i(\alpha)h(\alpha)+f_j(\alpha)k(\alpha)\equiv1(\text{mod }pO_k)$. 从而 $1=(p, f_i(\alpha), f_j(\alpha))=\mathfrak{p}_i+\mathfrak{p}_j=(\mathfrak{p}_i,\mathfrak{p}_j)$.

(C) $pO_K|\mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_g^{e_g}$. 这是由于：令 $\gamma_i=f_i(\alpha)$，则 $\mathfrak{p}_i=(p,\gamma_i)$. 由 (B) 知 $1\leqslant i\neq j\leqslant g$ 时，$(p,\gamma_i,\gamma_j)=1$. 令 $\mathfrak{a}=(p,\gamma_1^{e_1}\cdots\gamma_g^{e_g})$，则 $\mathfrak{p}_1\mathfrak{p}_2=(p,\gamma_1)(p,\gamma_2)=(p^2,p\gamma_1,p\gamma_2,\gamma_1\gamma_2)=(p(p,\gamma_1,\gamma_2),\gamma_1\gamma_2)=(p,\gamma_1\gamma_2)$. $\mathfrak{p}_1^2=(p,\gamma_1)^2=(p^2,p\gamma_1,\gamma_1^2)\subseteq(p,\gamma_1^2)$. 由此归纳下去即知 $\mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_g^{e_g}\subseteq(p,\gamma_1^{e_1}\cdots\gamma_g^{e_g})=\mathfrak{a}$. 只需再证 $\mathfrak{a}=pO_K$

即可．为此将 $x=\alpha$ 代入 $f(x)=f_1(x)^{e_1}\cdots f_g(x)^{e_g}(\mathrm{mod}\,p)$ 得到 $0=f(\alpha)\equiv f_1(\alpha)^{e_1}\cdots f_g(\alpha)^{e_g}=\gamma_1^{e_1}\cdots\gamma_g^{e_g}\ (\mathrm{mod}\,pO_K)$．即 $\gamma_1^{e_1}\cdots\gamma_g^{e_g}\in pO_K$．从而 $\mathfrak{a}=(p,\gamma_1^{e_1}\cdots\gamma_g^{e_g})=(p)=pO_K$.

现在证明定理 7 的(2)：由(A)我们不妨设 $\mathfrak{p}_1,\cdots,\mathfrak{p}_s$ 均不为 O_K，而 $\mathfrak{p}_{s+1}=\cdots=\mathfrak{p}_g=O_K$则 $\mathfrak{p}_i(1\leqslant i\leqslant s)$为$O_K$ 的素理想，$pO_k\subseteq\mathfrak{p}_i$，并且 $f(p/\mathfrak{p}_i)=f_i(1\leqslant i\leqslant s)$．由($B$)知 $\mathfrak{p}_1,\cdots,\mathfrak{p}_s$ 彼此不同．由(C)知 $pO_K|\mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_s^{e_s}$，于是 $pO_K=\mathfrak{p}_1^{d_1}\cdots\mathfrak{p}_s^{d_s}$，$d_i\leqslant e_i(1\leqslant i\leqslant s)$．利用引理 6 可知

$$n=d_1f_1+\cdots+d_sf_s\leqslant e_1f_1+\cdots+e_sf_s\leqslant e_1f_1+\cdots+e_gf_g.$$

但是由$f(x)\equiv f_1(x)^{e_1}\cdots f_g(x)^{e_g}\ (\mathrm{mod}\ p)$ 可知$n=\deg f=\sum_{i=1}^{g}e_i$

$\deg f_i(x)=\sum_{i=1}^{g}e_if_i$．于是只能是 $g=s$，并且 $e_i=d_i(1\leqslant i\leqslant g)$．这

就完成了定理 7 的证明．▌

注记 如果 O_K 中存在形如$\{1,\alpha,\cdots,\alpha^{n-1}\}$的整基，即 $O_K=\mathbf{Z}[\alpha]$，则$|O_K/\mathbf{Z}[\alpha]|=1$．从而对每个素数$p$均可用定理 7 的办法求 pO_K 的素理想分解式．我们在下节中会看到，每个二次域K 均有形如 $\{1,\alpha\}$ 的整基．但并不是每个域都可以这样作的（习题 1）．

例 3 $f(x)=x^3+x+1$ 是 $\mathbf{Q}[x]$中的不可约多项式，令 ω 是 $f(x)$在复数域上的一个根，则 $K=\mathbf{Q}(\omega)$ 为三次数域．经计算知 $\Delta(1,\omega,\omega^2)=-31$，没有平方因子，从而 $O_K=\mathbf{Z}[\omega]$．利用定理 7 我们可以得到任何素数 p 在 O_K 中素理想分解情况，比如：

对于 $p=2$，$f(x)(\mathrm{mod}\ 2)$无根，从而 $f(x)$在 $\mathbf{Z}/2\mathbf{Z}[x]$ 中仍不可约．因此 $2O_K$为 O_K 中素理想．

对于 $p=3$，$f(x)\equiv(x-1)(x^2+x-1)(\mathrm{mod}\ 3)$．而 x^2+x-1 在 $\mathbf{Z}/3\mathbf{Z}[x]$中不可约．于是 $3O_K=\mathfrak{p}_1\mathfrak{p}_2$，其中 $\mathfrak{p}_1=(3,\omega-1)$，

$\mathfrak{p}_2=(3,\omega^2+\omega-1)$是$O_K$中两个不同的素理想，并且$f(3/\mathfrak{p}_1)=1$，$f(3/\mathfrak{p}_2)=2$，即 $N(\mathfrak{p}_1)=3,N(\mathfrak{p}_2)=9$。

对于 $p=31,x^3+x+1\equiv(x-3)(x-14)^2(\bmod 31)$. 于是 $31O_K=\mathfrak{p}_1\mathfrak{p}_2^2,\mathfrak{p}_1=(31,\omega-3)$，$\mathfrak{p}_2=(31,\omega-14)$，$N(\mathfrak{p}_1)=N(\mathfrak{p}_2)=31$。

习 题

1．设 α 是$f(x)=x^3+5x+4=0$ 的一个根，$K=\mathbf{Q}(\alpha)$. 求证 K 为三次域(即$[K:\mathbf{Q}]=3$)，并且 $d(K)=-4\cdot 233$.

2．(Dedekind)(1) 证明 x^3+x^2-2x+8 为$\mathbf{Q}[x]$中不可约多项 式.

(2) 令 α 是该多项式的根，$K=\mathbf{Q}(\alpha)$. 证明 $\Delta(1,\alpha,\alpha^2)=4\cdot 503$.

(3) 证明 $\alpha'=4/\alpha\in O_K$，并且$\{1,\alpha,\alpha'\}$是O_K 的一组整基.

(4) 证明 $d(K)=503$.

(5) 证明对每个 $\gamma\in O_K$，$\{1,\gamma,\gamma^2\}$均不是O_K的整基.[提示：证明$\Delta(1,\gamma,\gamma^2)$是偶数.]

3．设$f(x)$是$\mathbf{Z}[x]$中不可约首一多项式，$\deg f=n,\alpha_1,\cdots,\alpha_n$ 是它的n个根. 求证：

(1) $\prod\limits_{1\leqslant r<s\leqslant n}(\alpha_r-\alpha_s)^2\in\mathbf{Z}$. 此数称作是多项式$f(x)$的判别式，记成$d_f$.

(2) 以$f'(x)$表示$f(x)$的导函数. 则 $d_f=(-1)^{\frac{n(n-1)}{2}}\prod\limits_{i=1}^{n}f'(\alpha_i)$.

(3) 令 $\alpha=\alpha_1,K=\mathbf{Q}(\alpha)$. 求证 $\Delta(1,\alpha,\cdots,\alpha^{n-1})=d_f$.

4．(1) 设 $f(x)=x^n+a$，$a\in\mathbf{Z}$. 求证 $d_f=(-1)^{\frac{n(n-1)}{2}}n^na^{n-1}$.

(2) 设 $f(x)=x^n+ax+b\in\mathbf{Z}[x]$ (不可约). 求证

$$d_f=(-1)^{\frac{n(n-1)}{2}}[(-1)^{n-1}(n-1)^{n-1}a^n+n^nb^{n-1}].$$

(3) 当(2)中取 $n=2$ 和 3，则 x^2+ax+b 和 x^3+ax+b 的判别式分别为a^2-4b 和$-(4a^3+27b^2)$(这就是通常所称的判别式).

5．复数 α 叫作是**单位根**，是指存在整数 $n\geqslant 1$ 使得$\alpha^n=1$.

(1) 求证：每个代数数域 K 中全部单位根形成一个乘法群，并且是有限循环群. [提示：设$[K:\mathbf{Q}]=n$，单位根 α 在 $\mathbf{Q}$ 上的极小多项式为 $x^m+a_1x^{m-1}+\cdots+a_m$，求证 $a_i\in\mathbf{Z}, m\leqslant n$，并且 $|a_i|\leqslant C_m^i(1\leqslant i\leqslant m)$. 由此可知 K 中只有有限多单位根. 而域中有限乘法群必为循环群].

(2) 若 $\alpha\in O_K$，则 α 是单位根$\Longleftrightarrow\alpha$ 的所有共轭元素的绝对值均为 1. [提示：令 $f_i(x)$ 为 α^i 在 $\mathbf{Q}$ 上的极小多项式. 证明 $\deg f_i(x)$ 和 $f_i(x)$ 诸系数的绝对值均有界，且此界只依赖$[K:\mathbf{Q}]$而不依赖 i. 于是 $f_i(x)(i\geqslant1)$ 只有有限个是不同的. 从而 $\alpha^i(i\geqslant1)$ 也是如此].

6. (1) 设 $\mathfrak{a}$ 是 O_K 的整理想，K 为代数数域，$N(\mathfrak{a})=g$. 求证 $g\in\mathfrak{a}$.

(2) 对于每个整数 $g\geqslant1$，求证在某个代数数域 K 中满足 $N(\mathfrak{a})\leqslant g$ 的整理想 $\mathfrak{a}$ 只有有限个.

7. 令 $K=\mathbf{Q}(\alpha), \alpha^3+\alpha^2-2\alpha+8=0$（习题 2）. 求出素数 3,5 和 503 在 O_K 中的素理想分解式.

§6.5 二 次 域

现在我们将上节的一般性结果用于二次域. 所谓二次域 K 即是有理数域 $\mathbf{Q}$ 的二次扩张. 于是 $K=\mathbf{Q}(\alpha)$，其中 α 是某个不可约多项式 $x^2+ax+b\in\mathbf{Z}[x]$ 的根. 于是 $\alpha=\frac{1}{2}(-a\pm\sqrt{a^2-4b})$，$\sqrt{a^2-4b}\notin\mathbf{Q}$. 但这时 $K=\mathbf{Q}(\alpha)=\mathbf{Q}(\sqrt{a^2-4b})$. 如果 $a^2-4b=n^2d$，则 $K=\mathbf{Q}(\sqrt{d})$. 因此每个二次域总可写成为：

$K=\mathbf{Q}(\sqrt{d}), \sqrt{d}\notin\mathbf{Z}, d\in\mathbf{Z}$，并且 d 没有平方因子.

我们先来决定二次域的整数环.

定理 8 设 $K=\mathbf{Q}(\sqrt{d})$ 是二次域，$d\in\mathbf{Z}$，d 无平方因子.

(1) 对于元素 $\alpha\in K$，则：$\alpha\in O_K\Longleftrightarrow T(\alpha), N(\alpha)\in\mathbf{Z}$.

(2) 令 $$\omega=\begin{cases}\frac{1}{2}(1+\sqrt{d}),\text{当 } d\equiv1 \pmod 4\text{ 时},\\ \sqrt{d},\text{当 } d\equiv2,3 \pmod 4\text{ 时}.\end{cases}$$

则$\{1,\omega\}$为 O_K 的一组整基，即 $O_K=\mathbf{Z}[\omega]=\mathbf{Z}\oplus\mathbf{Z}\omega$.

(3) $d(K)=\begin{cases} d, \text{当 } d\equiv 1 \pmod 4 \text{时},\\ 4d, \text{当 } d\equiv 2,3 \pmod 4 \text{时}. \end{cases}$

证明 (1) $\Rightarrow$显然. $\Leftarrow$是因为 α 是首一多项式 $x^2-T(\alpha)x+N(\alpha)\in\mathbf{Z}[x]$的根.

(2)和(3)：当$d\equiv 1 \pmod 4$时. 由于$T\left(\frac{1}{2}(1+\sqrt{d})\right)=1$, $N\left(\frac{1}{2}(1+\sqrt{d})\right)=\frac{1}{4}(1-d)\in\mathbf{Z}$. 从而由(1)知$\frac{1}{2}(1+\sqrt{d})\in O_K$. 又由于

$$\left\{1,\frac{1}{2}(1+\sqrt{d})\right\}\text{的判别式}=\begin{vmatrix}1 & \frac{1}{2}(1+\sqrt{d})\\ 1 & \frac{1}{2}(1-\sqrt{d})\end{vmatrix}^2=d.$$

而d无平方因子，于是$\left\{1,\frac{1}{2}(1+\sqrt{d})\right\}$是$O_K$的整基，并且$d(K)=d$.

若$d\equiv 2,3 \pmod 4$. K中元素均可唯一表成$\alpha+\beta\sqrt{d}$，α, $\beta\in\mathbf{Q}$. 由(1)知$\alpha+\beta\sqrt{d}\in O_K\Longleftrightarrow 2\alpha, \alpha^2-\beta^2 d\in\mathbf{Z}$，这时$(2\alpha)^2-(2\beta)^2 d\in 4\mathbf{Z}$，从而$(2\beta)^2 d\in\mathbf{Z}$. 由于$d$无平方因子，从而$2\beta\in\mathbf{Z}$. 令$2\alpha=a$, $2\beta=b$，则$a,b\in\mathbf{Z}$，并且$a^2-b^2d\equiv 0 \pmod 4$. 当$d\equiv 2,3 \pmod 4$时，不难看出$a^2-b^2d\equiv 0 \pmod 4$的解必然满足$a,b\in 2\mathbf{Z}$. 于是$\alpha,\beta\in\mathbf{Z}$. 反之，如果$\alpha$, $\beta\in\mathbf{Z}$，则显然$\alpha+\beta\sqrt{d}\in O_K$. 从而$O_K=\{\alpha+\beta\sqrt{d}\mid\alpha, \beta\in\mathbf{Z}\}=\mathbf{Z}\oplus\mathbf{Z}\sqrt{d}=\mathbf{Z}[\sqrt{d}]$，即$\{1,\sqrt{d}\}$是$O_K$的整基，而$d(K)=\begin{vmatrix}1 & \sqrt{d}\\ 1 & -\sqrt{d}\end{vmatrix}^2=4d$. ▌

下一步要研究素数p在二次域整数环O_K中素理想分解的情形. 由引理6证明的关系式$\sum_{i=1}^{g}e_i f_i=2$，可知p在二次域整数环O_K中的分解只能有以下三种可能.

(A) $pO_K=\mathfrak{p}_1\mathfrak{p}_2, \mathfrak{p}_1\neq\mathfrak{p}_2, N(\mathfrak{p}_1)=N(\mathfrak{p}_2)=p$.

(B) $pO_K=\mathfrak{p}^2, N(\mathfrak{p})=p$,

(C) $pO_K=\mathfrak{p}$,即 pO_K 为 O_K 中素理想,此时 $N(\mathfrak{p})=p^2$.

为了判别 pO_K 的分解究竟属于哪种情形,我们需要初等数论中的一个符号：Legendre 符号．设 p 是奇素数，$n\in\mathbf{Z}$，并且 $p\nmid n$．如果 $x^2\equiv n \pmod p$ 有解,则称 n **是模 p 的二次剩余**,并且表示成 $\left(\frac{n}{p}\right)=1$．如果同余方程 $x^2\equiv n \pmod p$ 无解，则称 n 为模 p 的**二次非剩余**,表示成 $\left(\frac{n}{p}\right)=-1$．不难证明，两个二次剩余之积仍是二次剩余,一个二次剩余和一个二次非剩余之积为二次非剩余,而两个二次非剩余之积是二次剩余．从而映射

$$\left(\frac{}{p}\right):(\mathbf{Z}/p\mathbf{Z}-\{0\})\to\{\pm1\}, n\mapsto\left(\frac{n}{p}\right)$$

是乘法群的同态．模 p 的二次剩余共有 $\frac{p-1}{2}$ 个,即是 $1^2, 2^2, \cdots, \left(\frac{p-1}{2}\right)^2$ 的模 p 同余类,从而二次非剩余也有 $\frac{p-1}{2}$ 个同余类．对于大素数 p，由定义来判别 n 是二次剩余还是二次非剩余是不方便的.但是在初等数论中给出计算 Legendre 符号 $\left(\frac{n}{p}\right)$ 的好方法,即二次互反律．详见有关初等数论的书.

定理 9 设 $K=\mathbf{Q}(\sqrt{d})$ 为二次域, d 为无平方因子的整数, p 为素数.

(1) 如果 $p\mid d(K)$,则 $pO_K=\mathfrak{p}^2$.

(2) 若 p 为奇素数并且 $p\nmid d(K)$(这时必然 $p\nmid d$),则

当 $\left(\frac{d}{p}\right)=1$ 时, $pO_K=\mathfrak{p}_1\mathfrak{p}_2, \mathfrak{p}_1\neq\mathfrak{p}_2$.

当 $\left(\frac{d}{p}\right)=-1$ 时, $pO_K=\mathfrak{p}$.

(3) 若 $p=2$,且 $2\nmid d(K)$(这时必然 $d\equiv 1\pmod 4$),则

当 $d\equiv 1\pmod 8$时,$2O_K=\mathfrak{p}_1\mathfrak{p}_2,\mathfrak{p}_1\neq\mathfrak{p}_2$.

当 $d\equiv 5\pmod 8$时,$2O_K=\mathfrak{p}$.

证明 由定理 8 知 O_K 有形如$\{1,\omega\}$的整基,从而对每个素数 p 均可用定理 7 来求 pO_K 分解情况.

(a) 设$d\equiv 2,3\pmod 4$. 这时 $\omega=\sqrt{d}$, ω 的极小多项式为 $f(x)=x^2-d$, $d(K)=4d$.

先设 p 为奇素数. 这时在 $p|d(K)=4d$ 即 $p|d$ 时, $f(x)\equiv x^2\pmod p$. 于是 $pO_K=\mathfrak{p}^2,\mathfrak{p}=(p,\sqrt{d})$. 当 $p\nmid d(K)=4d$ 即 $p\nmid d$ 时,如果$\left(\frac{d}{p}\right)=1$,即有 $a\in\mathbf{Z}$ 使得 $d\equiv a^2\pmod p$, 则 $f(x)=x^2-d\equiv(x-a)(x+a)\pmod p$, 并且 $a\not\equiv -a\pmod p$, 从而 $x-a$ 和 $x+a$ 是 $\mathbf{Z}/p\mathbf{Z}[x]$中不同的多项式. 因此 $pO_K=\mathfrak{p}_1\mathfrak{p}_2$, $\mathfrak{p}_1\neq\mathfrak{p}_2$, $\mathfrak{p}_1=(p,\sqrt{d}-a)$, $\mathfrak{p}_2=(p,\sqrt{d}+a)$. 如果$\left(\frac{d}{p}\right)=-1$,则 $f(x)=x^2-d$ 为模 p 不可约多项式,从而 $pO_K=\mathfrak{p}$.

再设 $p=2$. 这时 $p|d(K)=4d$. 当 $d\equiv 2\pmod 4$时, $f(x)=x^2-d\equiv x^2\pmod 2$,从而 $2O_K=\mathfrak{p}^2,\mathfrak{p}=(2,\sqrt{d})$. 而当 $d\equiv 3\pmod 4$时,$f(x)=x^2+1\equiv(x+1)^2\pmod 2$,从而 $2O_K=\mathfrak{p}^2$, $\mathfrak{p}=(2,\sqrt{d}+1)$.

(b) 设$d\equiv 1\pmod 4$. 这时 $\omega=\frac{1}{2}(1+\sqrt{d})$. 它的极小多项式为 $x^2-x-\frac{1}{4}(d-1)\in\mathbf{Z}[x]$. $d(K)=d$.

先设 p 为奇素数. 我们不用 $O_K=\mathbf{Z}[\omega]$而仍用环 $\mathbf{Z}[\sqrt{d}]$. 由于$|O_K/\mathbf{Z}[\sqrt{d}]|=2$, 于是 $p\nmid|O_K/\mathbf{Z}[\sqrt{d}]|$. 从而利用定理 7 可知其结论与 $d\equiv 2,3\pmod 4$时完全相同.

再设 $p=2$. 当 $d\equiv 1\pmod 8$时,$x^2-x-\frac{1}{4}(d-1)\equiv x(x-$

$1)\pmod 2$. 于是 $2O_K=\mathfrak{p}_1\mathfrak{p}_2$, $(2,\omega)=\mathfrak{p}_1\neq\mathfrak{p}_2=(2,\omega-1)$. 最后当 $d\equiv5\pmod 8$时, $x^2-x-\frac{1}{4}(d+1)\equiv x^2+x+1\pmod 2$,而 x^2+x+1 是 mod 2 不可约多项式,因此 $2O_K=\mathfrak{p}$. ▌

现在介绍一下关于二次域的理想类数问题. Gauss 最早研究了二次域 $K=\mathbf{Q}(\sqrt{-1})$的理想类数,证明了 $h(K)=1$. 即 O_K 是主理想整环. 其证明完全是仿照 $\mathbf{Z}$ 中所采用的方法. 大家知道,证明 $\mathbf{Z}$ 为主理想整环的通常办法是借助于欧几里德除法算式:对于任意整数 n 和正整数 m, 均存在 $q,r\in\mathbf{Z}$, 使得 $n=qm+r$, $0\leqslant r<m$ (q 为商数, r 为余数). Gauss 将欧氏除法算式推广到 $\mathbf{Z}[\sqrt{-1}]$中,其形式是:

引理 7 设 $a+b\sqrt{-1}$, $c+d\sqrt{-1}\in\mathbf{Z}[\sqrt{-1}]$(即 $a,b,c,d\in\mathbf{Z}$), 并且 $c+d\sqrt{-1}\neq0$. 则有 $A+B\sqrt{-1}$, $C+D\sqrt{-1}\in\mathbf{Z}[\sqrt{-1}]$,使得

$$a+b\sqrt{-1}=(c+d\sqrt{-1})(A+B\sqrt{-1})+(C+D\sqrt{-1}),$$

并且 $0\leqslant N(C+D\sqrt{-1})=C^2+D^2<N(c+d\sqrt{-1})$.

证明 $\dfrac{a+b\sqrt{-1}}{c+d\sqrt{-1}}=\alpha+\beta\sqrt{-1}\in K=\mathbf{Q}(\sqrt{-1})$, 即 $\alpha,\beta\in\mathbf{Q}$. 令 A 和 B 分别是距 α,β 最近的整数,则对于 $\gamma=\alpha-A$ 和 $\delta=\beta-B$,便有 $|\gamma|\leqslant1/2$, $|\delta|\leqslant1/2$. 于是 $N(\gamma+\delta\sqrt{-1})=\gamma^2+\delta^2\leqslant\frac{1}{4}+\frac{1}{4}<1$. 而

$$a+b\sqrt{-1}=(c+d\sqrt{-1})(A+B\sqrt{-1})+(c+d\sqrt{-1})(\gamma+\delta(\sqrt{-1})).$$

取 $C+D\sqrt{-1}=(c+d\sqrt{-1})(\gamma+\delta\sqrt{-1})$, 则 $C+D\sqrt{-1}=a+b\sqrt{-1}-(c+d\sqrt{-1})(A+B\sqrt{-1})\in\mathbf{Z}[\sqrt{-1}]$, 并且 $0\leqslant N(C+D\sqrt{-1})=N(c+d\sqrt{-1})\cdot N(\gamma+\delta\sqrt{-1})<N(c+$

$d\sqrt{-1}$). ▌

系 $\mathbf{Z}[\sqrt{-1}]$是主理想整环．因此二次域$\mathbf{Q}(\sqrt{-1})$的理想类数为1．

证明 设$\mathfrak{a}$是$\mathbf{Z}[\sqrt{-1}]$中非零理想．命$c+d\sqrt{-1}$是$\mathfrak{a}$中范最小的非零元素，则对于每个$a+b\sqrt{-1}\in\mathfrak{a}$，由引理7我们有$a+b\sqrt{-1}=(c+d\sqrt{-1})(A+B\sqrt{-1})+(C+D\sqrt{-1})$，$A,B,C,D\in\mathbf{Z}$．并且$N(C+D\sqrt{-1})<N(c+d\sqrt{-1})$．显然$C+D\sqrt{-1}\in\mathfrak{a}$．于是只可能$C+D\sqrt{-1}=0$．即$a+b\sqrt{-1}\in(c+d\sqrt{-1})$．从而$\mathfrak{a}=(c+d\sqrt{-1})$，即$\mathfrak{a}$为主理想．▌

用上述方法只能决定很有限的几个二次域的理想类数．Gauss得到了任意二次域理想类数的一个公式．利用这个公式，Gauss手算了许多二次域的理想类数．基于这些数据Gauss提出了两个著名的猜想：

（一）只有有限多个虚二次域$\mathbf{Q}(\sqrt{d})$（即$d<0$）的理想类数是1．他猜想只有9个理想类数为1的虚二次域，即$d=-1,-2,-3,-7,-11,-19,-43,-67$和$-163$．这个猜想一直到1967年才由美国数学家Stark和英国数学家Baker各自独立地证明．

（二）存在着无限多个实二次域$\mathbf{Q}(\sqrt{d})$（即$d>0$）的理想类数是1．这个猜想至今既没有证明也没有被推翻．

作为定理9的应用，我们看一下当年Gauss如何用二次域$\mathbf{Q}(\sqrt{-1})$的整数环$\mathbf{Z}[\sqrt{-1}]$来解决初等数论中的二平方和问题（后人把$\mathbf{Z}[\sqrt{-1}]$称作是高斯整数环）．这个问题是：

哪些自然数可以表示成两个整数的平方和？

由于$n=a^2+b^2\Longleftrightarrow n=N(a+b\sqrt{-1})$．这就把二平方和问题与高斯整数环$\mathbf{Z}[\sqrt{-1}]$联系起来．

定理 10（Gauss，二平方和定理） 设n为正整数，$n=m^2n_0$，

其中 $m\in \mathbf{Z}$ 而 n_0 没有平方因子. 则: n 可表成二个整数的平方和$\Longleftrightarrow n_0$ 没有素因子 $p\equiv 3 \pmod 4$.

证明 $\Leftarrow$: 首先注意, 如果 n_1 和 n_2 均可表成两个整数的平方和,则 n_1n_2 也可如此. 这是因为: 若 $n_1=a^2+b^2$, $n_2=c^2+d^2$, 则 $n_1=N(a+b\sqrt{-1})$, $n_2=N(c+d\sqrt{-1})$, 从而 $n_1n_2=N((a+b\sqrt{-1})(c+d\sqrt{-1}))=N((ac-bd)+(ad+bc)\sqrt{-1})=(ac-bd)^2+(ad+bc)^2$. 因此,为证 n 可表成二平方和, 只需证明其无平方因子部分 n_0 的每个素因子可表成二平方和即可. 根据假设可知 $n_0=p_1\cdots p_s$, 其中 $p_1,\cdots,p_s$ 为两不同的素数, 并且 $p_i=2$ 或者 $p_i\equiv 1 \pmod 4$. 如果 $p_i=2$, 则 $2=1^2+1^2$. 如果 $p_i\equiv 1 \pmod 4$, 由初等数论知道 $\left(\frac{-1}{p_i}\right)=1$ (事实上不难证明 $\left(\left(\frac{p_i-1}{2}\right)!\right)^2\equiv -1 \pmod{p_i}$). 于是由定理 8 可知在 $O_K=\mathbf{Z}[\sqrt{-1}]$中, $p_iO_K=\mathfrak{p}_1\mathfrak{p}_2$, $N(\mathfrak{p}_1)=N(\mathfrak{p}_2)=p_i$. 由引理 7 的系知 $\mathbf{Z}[\sqrt{-1}]$ 是主理想整环. 因此 $\mathfrak{p}_1=(a+b\sqrt{-1})$, $a,b\in\mathbf{Z}$. 从而 $p_i=N(\mathfrak{p}_1)=N(a+b\sqrt{-1})=a^2+b^2$. 这说明 n_0 的每个素因子均可表成二平方和,从而 n_0 和 n 均可如此.

$\Rightarrow$: 假设 n 可表成二平方和,则 $\mathbf{Z}[\sqrt{-1}]$ 中存在理想 $\mathfrak{a}$ 使得 $N(\mathfrak{a})=n$. 如果存在素数 $p\equiv 3 \pmod 4$ 使得 $p\mid n_0$,则 $n=m^2n_0$中包含 p 的奇次幂. 但是另一方面, 初等数论中证明了: 当 $p\equiv 3 \pmod 4$时, $\left(\frac{-1}{p}\right)=-1$. 从而由定理 8 可知 $pO_K=\mathfrak{p}$ 为$\mathbf{Z}[\sqrt{-1}]$中素理想,并且 $\mathfrak{p}$ 也显然是 $\mathbf{Z}[\sqrt{-1}]$ 中唯一的素理想使得 $p\mid N(\mathfrak{p})$. 因此,若令 $\mathfrak{a}$ 的素理想分解式中 $\mathfrak{p}$ 的幂次为 $e\geqslant 0$, 则 $n=N(\mathfrak{a})=N(\mathfrak{p})^e\cdots=p^{2e}\cdots$.即 n 的分解式中 p 出现偶次幂.这就与前述 n 中 p 出现奇次方幂相矛盾. 从而 n_0不可能有素因子 $p\equiv 3 \pmod 4$. ▌

在历史上，除了二次域之外，还有一类数域被研究得较为深入，这就是分圆域. Kummer 在上世纪中期对于分圆域的开创性工作直接受到 Fermat 猜想的推动. 近代分圆域理论的奠基人是 K. Iwasawa（岩泽健吉），他使用了相当深刻的交换代数手段. Fermat 问题与代数几何有着密切联系. 这是因为 $x^n+y^n=z^n$ 具有整数解 $xyz\neq0$ 和方程 $X^n+Y^n=1$ 具有有理数解显然是等价的. 1922 年，英国数学家 Mordell 提出一个大胆的猜想：设 $f(x,y)$ 是 $\mathbf{Q}[x,y]$ 中不可约多项式. 如果不可约平面曲线 $f(x,y)=0$ 的亏格 $\geqslant2$，则 $f(x,y)=0$ 只有有限个有理数解. 这个猜想于1983年由 29 岁的德国年青数学家 Faltings 所证明（利用了大量代数几何知识），这项结果被认为是本世纪数学最杰出的成就之一. 在代数几何中证明了曲线 $x^n+y^n=1$ 的亏格是 $\frac{1}{2}(n-1)(n-2)$. 当 $n\geqslant4$ 时，其亏格 $\geqslant2$. 所以作为 Faltings 结果的直接推论，当 $n\geqslant4$ 时，$x^n+y^n=1$ 至多只有有限个有理解，于是Fermat方程 $x^n+y^n=z^n$ 在 $n\geqslant4$ 时至多只有有限个整数解 $xyz\neq0$. 这些进展更充分表明代数几何与数论之间具有深刻的联系.

习　题

1. 设 $K=\mathbf{Q}(\sqrt{-5})$. 求素数 $p=2,3,5,7,11,13$ 在 O_K 中的素理想分解式. 再对 $K=\mathbf{Q}(\sqrt{5})$ 作同样事情.

2. 试问何种正整数 n 可表成形式 $n=a^2+3b^2(a,b\in\mathbf{Z})$？［提示：利用 $\mathbf{Z}\left[\frac{1}{2}(1+\sqrt{-3})\right]$ 的理想类数为 1 这个事实，见习题 6.］

3. 求证对每个二次域 K，$O_K=\mathbf{Z}\oplus\mathbf{Z}\cdot\left(\frac{d(K)+\sqrt{d(K)}}{2}\right)$.

4. (1) 求证实二次域的单位根群为 $\{\pm1\}$.

(2) 如果 $d<-3$，求证虚二次域 $\mathbf{Q}(\sqrt{d})$ 的单位根群为 $\{\pm1\}$.

(3) 决定$\mathbf{Q}(\sqrt{-1})$和$\mathbf{Q}(\sqrt{-3})$的单位根群.

5. (1) 对于$K=\mathbf{Q}(\sqrt{10})$和$\mathbf{Q}(\sqrt{-5})$，求6在O_K中的素理想分解式.

(2) 证明$\mathbf{Z}[\sqrt{10}]$和$\mathbf{Z}[\sqrt{-5}]$均不是主理想整环.

6. 模仿引理7和它的系，证明$\mathbf{Z}\left[\frac{1}{2}(1+\sqrt{-3})\right]$是主理想整环.

第七章　分次环，维数理论和完备化方法

分次模和分次环的背景是代数几何中的射影代数簇．将分次环自然地引进拓扑之后，自然就产生了分次环对于拓扑的完备化问题．例如，形式幂级数环是多项式环对于自然分次和相应拓扑的完备化．从 Weierstrass 和 Riemann 以来，形式幂级数环就是研究代数簇局部特性的基本工具，形成代数几何中的解析方法．最后，关于环的维数理论也是在代数几何中研究代数簇维数的基础上发展起来的．目前，分次和维数概念以及完备化方法已成为研究环和模特性的基本手段．

本章共分三节．第一节讲分次环和分次模，并介绍有限生成分次模的 Hilbert 多项式．第二节介绍 Noether 局部环的维数理论和它在代数几何中的应用．第三节讲分次环的 $\mathfrak{a}$-adic 拓扑和完备化方法．在这节中我们需要一些点集拓扑的基本知识．

§7.1　分次环和分次模

定义　(具有幺元素的交换)环 A 叫作是**分次环**，是指满足以下两个条件：

(1) 作为加法群 A 是可数无穷多子群的直和，$A=\bigoplus\limits_{n=0}^{\infty}A_n$；

(2) 对于乘法，则 $A_nA_m\subseteq A_{n+m}(n,m\geqslant 0)$．

于是，A 中每个元素均唯一地表示成

$a=(a_0,a_1,\cdots,a_n,\cdots)$，$a_n\in A_n$，只有有限多个 $a_n\neq 0$．

我们把元素 $a_n\in A_n$ 和 A 中元素$(0,\cdots,0,a_n,0,0,\cdots)$等同，而称 a_n 是 a 的 n 次齐次分量，而 A_n 称作是环 A 的 n 次齐次分量．不难看出，A_0 为 A 的子环，而每个 A_n 均是 A_0-模．并且对每个

$i \geqslant 0$，$\bigoplus\limits_{n=i}^{\infty} A_n$ 均为 A 的理想．特别地，$A_+ = \bigoplus\limits_{n=1}^{\infty} A_n$ 为 A 的理想，而 $A = A_0 \oplus A_+$．最后，A 是 A_0 上的交换代数．

例 1 设 R 为环，$A = R[x_1, \cdots, x_r]$为 R 上关于 $x_1, \cdots, x_r$ 的多项式环．取 A_n 为 A 中全部 n 次齐次多项式和零所组成的加法子群．则 $A = \bigoplus\limits_{n=0}^{\infty} A_n$ 为分次环，其中 $A_0 = R$．对于 A 中每个多项式 $f(x_1, \cdots, x_r)$，它的 n 次齐次分量就是该多项式的 n 次齐次部分，而 A_+ 是由 $x_1, \cdots, x_r$ 所生成的理想．

例 2 $A = \mathbf{Z}[x^2, x^3]$．令 $A_0 = \mathbf{Z}, A_1 = (0)$，对于 $n \geqslant 2$，由于 $2a + 3b = n$ 一定有非负整解(a, b)，从而 $x^n = (x^2)^a (x^3)^b \in A$．于是若令 $A_n = \mathbf{Z}x^n (n \geqslant 2)$，则 $A = \bigoplus\limits_{n=0}^{\infty} A_n$ 为分次环．

例 3 设 A 为环，$\mathfrak{a}$ 为 A 的理想．考虑加法 Abel 群 $\mathfrak{a}^n$的直和：

$$A^* = \bigoplus_{n=0}^{\infty} \mathfrak{a}^n \quad (\mathfrak{a}^0 = A).$$

利用环 A 中的乘法自然定义 A^* 中的乘法．即若 $x, y \in A^*$，$x = (x_0, x_1, \cdots, x_n, \cdots), y = (y_0, y_1, \cdots, y_n, \cdots), x_n, y_n \in \mathfrak{a}^n (n \geqslant 0)$．我们定义

$$xy = (z_0, z_1, \cdots, z_n, \cdots),$$

$$z_n = \sum_{i=0}^{n} x_i y_{n-i} \in \mathfrak{a}^n.$$

不难看出，A^* 是一个分次环，其中 $\mathfrak{a}^n$ 为 A^* 的 n 次齐次分量．

例 4 设 A 为环，$\mathfrak{a}$ 为 A 的理想．考虑加法群 $\mathfrak{a}^n/\mathfrak{a}^{n+1} (n \geqslant 0)$ 的直和

$$G_{\mathfrak{a}}(A) = \bigoplus_{n=0}^{\infty} \mathfrak{a}^n/\mathfrak{a}^{n+1}.$$

对于 $x_n \in \mathfrak{a}^n$，我们以 $\bar{x}_n$ 表示 $\mathfrak{a}^n/\mathfrak{a}^{n+1}$ 中对应的元素．对于 $\bar{x}_n \in$

$\mathfrak{a}^n/\mathfrak{a}^{n+1}$ 和 $\bar{x}_m \in \mathfrak{a}^m/\mathfrak{a}^{m+1}$，我们定义

$$\bar{x}_n \cdot \bar{x}_m = \overline{x_n x_m} \in \mathfrak{a}^{n+m}/\mathfrak{a}^{n+m+1}$$

不难验证，这个乘法是可定义的，即与代表元 x_n 和 x_m 的不同选取方式无关. 将此乘法按自然方式扩充到整个 $G_\mathfrak{a}(A)$ 上，即对于 $x, y \in G_\mathfrak{a}(A)$，$x = (\bar{x}_0, \bar{x}_1, \cdots, \bar{x}_n, \cdots)$，$y = (\bar{y}_0, \bar{y}_1, \cdots, \bar{y}_n, \cdots)$，$\bar{x}_n, \bar{y}_n \in \mathfrak{a}^n/\mathfrak{a}^{n+1}$ $(x \geqslant 0)$，我们定义

$$xy = (\bar{z}_0, \bar{z}_1, \cdots, \bar{z}_n, \cdots),$$

$$z_n = \sum_{i=0}^{n} x_{n-i} y_i \in \mathfrak{a}^n.$$

则 $G_\mathfrak{a}(A)$ 由此形成分次环.

定义 设 $A = \bigoplus_{n=0}^{\infty} A_n$ 是分次环. A-模 M 叫作是**分次 A-模**，是指满足以下两个条件：

(1) M 是可数无穷多个 A-子模的直和，$M = \bigoplus_{n=0}^{\infty} M_n$；

(2) $A_m M_n \subseteq M_{m+n}$ $(m, n \geqslant 0)$.

这时，易知每个 M_n 均是 A_0-模，并且 M 中元素均唯一表示成

$$y = (y_0, y_1, \cdots, y_n, \cdots), \quad y_n \in M_n, \quad 有限个\ y_n \neq 0.$$

y_n 叫作是 y 的 **n 次齐次分量**，M_n 叫作是分次模 M 的 n 次齐次分量. 如果把 $y_n \in M_n$ 与 M 中元素 $(0, \cdots, 0, y_n, 0, \cdots)$ 等同，则称 M_n 中元素 y_n 为 M 中的**齐次元素**，次数为 n，表示成 $\deg y_n = n$.

例 5 每个分次环 $A = \bigoplus_{n=0}^{\infty} A_n$ 本身是分次 A-模 $(M = A, M_n = A_n)$.

例 6 设 A 为环而 $\mathfrak{a}$ 是 A 的理想. 我们在例 3 中构作了分次环 $A^* = \bigoplus_{n=0}^{\infty} \mathfrak{a}^n$. 对于每个 A-模 M，$M_n = \mathfrak{a}^n M$ 为 M 的 A-子

模．考虑它们的直和

$$M^{*}=\bigoplus_{n=0}^{\infty}\mathfrak{a}^{n}M,$$

自然定义 A^{*} 在 M^{*} 上的作用，即对于 $a=(a_0,\cdots,a_n,\cdots)\in A^{*}$，$a_n\in\mathfrak{a}^n$，$x=(x_0,\cdots,x_n,\cdots)\in M^{*}$，$x_n\in\mathfrak{a}^nM$，定义

$$ax=(y_0,\cdots,y_n,\cdots),$$

$$y_n=\sum_{i=0}^{n}a_ix_{n-i}\in\mathfrak{a}^nM.$$

不难验证，M^{*} 由此而成为分次 A^{*}-模．叫作是由 M 构作出的 $\mathfrak{a}$-分次模．

定义 设 $\mathfrak{a}$ 为环 A 的理想，M 为 A-模．对于 M 的 A-子模降链

$$(*)\quad M=M_0\supseteq M_1\supseteq\cdots\supseteq M_n\supseteq\cdots$$

如果 $\mathfrak{a}M_n\subseteq M_{n+1}$（对每个 $n\geqslant 0$），则称（$*$）是一个 $\mathfrak{a}$-链．进而，如果又存在 n_0，使得 $n\geqslant n_0$ 时均有 $\mathfrak{a}M_n=M_{n+1}$，则称（$*$）是稳定的 $\mathfrak{a}$-链．例如 $M_n=\mathfrak{a}^nM\,(n\geqslant 0)$ 就是最简单的稳定 $\mathfrak{a}$-链．而例 6 可以推广成

例 7 设（$*$）是 A-模 M 的子模 $\mathfrak{a}$-链，则 $M^{*}=\bigoplus_{n}^{\infty}M_n$ 对于自然的运算为 $A^{*}=\bigoplus_{n=0}^{\infty}\mathfrak{a}^n$ 上的分次模．

例 8 设 $\mathfrak{a}$ 为环 A 的理想．我们在例 4 中已经定义了分次环 $G_{\mathfrak{a}}(A)=\bigoplus_{n=0}^{\infty}\mathfrak{a}^n/\mathfrak{a}^{n+1}$．如果（$*$）为 A-模 M 的子模 $\mathfrak{a}$-链，考虑 Abel 群

$$G_{\mathfrak{a}}(M)=\bigoplus_{n=0}^{\infty}M_n/M_{n+1}.$$

对于 $\bar{a}_n\in\mathfrak{a}^n/\mathfrak{a}^{n+1}$，$\bar{x}_m\in M_m/M_{m+1}$，定义 $\bar{a}_n\cdot\bar{x}_m=\overline{a_nx_m}\in M_{n+m}$

$/M_{n+m+1}$. 由于$\{M_n\}$是$\mathfrak{a}$-链可知这个乘法是可定义的，即与代表元 a_n 和 x_m 的选取方式无关. 将此乘法自然扩充成 $G_\mathfrak{a}(A)$ 中任意元素与 $G_\mathfrak{a}(M)$ 中任意元素的乘法. 可知 $G_\mathfrak{a}(M)$ 由此而成为分次 $G_\mathfrak{a}(A)$-模.

现在研究分次环和分次模的有限生成特性. 首先研究分次环何时为 Noether 环.

引理 1 设 $A=\bigoplus\limits_{n=0}^{\infty}A_n$ 为分次环. 则: A 为 Noether 环$\Longleftrightarrow$ A_0 为 Noether 环并且 A 为有限生成 A_0-代数.

证明 $\Leftarrow$: 如果 A_0 为 Noether 环而 A 为有限生成 A_0-代数，则 $A=A_0[u_1,\cdots,u_s]$, $u_i\in A$. 从而A是多项式环$A_0[x_1,\cdots,x_n]$的商环. 由于 A_0 为 Noether 环，从而 $A_0[x_1,\cdots,x_s]$为 Noether 环(Hilbert 基定理)，于是其商环 A 也是 Noether 环.

$\Rightarrow$: 如果 A 为 Noether 环，则商环 $A_0\cong A/A_+$ 也是 Noether 环. 另一方面，A_+ 作为 A 的理想是有限生成的. 设 $A_+=Au_1+\cdots+Au_s$, $u_i\in A$, 将每个 u_i 表示成有限个齐次分量之和，不难看出，u_i 的零次分量为 0 $(1\leqslant i\leqslant s)$，而 A_+ 也是由 $u_i(1\leqslant i\leqslant s)$的全部齐次分量所生成的. 于是我们从一开始就可不妨假定 $u_1,\cdots,u_s$ 均是次数$\geqslant1$ 的齐次元素. 令$\deg u_i=k_i\geqslant1(1\leqslant i\leqslant s)$. 记 $A'=A_0[u_1,\cdots,u_s]$，则 $A'\subseteq A$. 我们现在对 n 归纳证明 $A_n\subseteq A'$: 显然 $A_0\subseteq A'$. 现在设 $n\geqslant1$ 而 $y_n\in A_n$. 由于 $A_n\subseteq A_+=Au_1+\cdots+Au_s$, 从而$y_n=\sum\limits_{i=1}^{s}a_iu_i$, $a_i\in A_{n-k_i}$(当 $m<0$ 时我们规定 $A_m=(0)$). 由于 $k_i\geqslant1$，根据归纳假设知 $a_i\in A'(1\leqslant i\leqslant s)$，于是 $y_n=\sum\limits_{i=1}^{s}a_iu_i\in A'$. 这就证明了对于每个 $n\geqslant0$ 均有 $A_n\subseteq A'$. 于是 $A=A'=A_0[u_1,\cdots,u_s]$. 即 A 是有限生成 A_0-代数. ▌

系 设 A 为 Noether 环，$\mathfrak{a}$ 为 A 的理想. 则分次环 $A^* = \bigoplus_{n=0}^{\infty} \mathfrak{a}^n$ 是 Noether 环.

证明 设 $\mathfrak{a} = Au_1 + \cdots + Au_s$ (Noether 环 A 的理想 $\mathfrak{a}$ 是有限生成的)，则作为 $A = \mathfrak{a}^0$ 上的代数，A^* 显然是由 $u_1, \cdots, u_s$ 有限生成的. 由引理 1 即知 A^* 为Noether 环. ▌

引理 2 设 A 为 Noether 环，$\mathfrak{a}$ 为 A 的理想. M 为有限生成 A-模，$\{M_n\}$是 M 的子模 $\mathfrak{a}$-链. 则：$M^* = \bigoplus_{n=0}^{\infty} M_n$为有限生成 A^*-模$\Longleftrightarrow\{M_n\}$为稳定的 $\mathfrak{a}$-链.

证明 由于 A 为 Noether 环而 M 为有限生成 A-模，所以 M 为 Noether A-模. 于是子模 M_n 均为有限生成 A-模. 从而 $Q_n = \bigoplus_{k=0}^{n} M_k$ 也是有限生成 A-模. 但是 Q_n 不一定是 A^*-模. 不难看出，Q_n 所生成的 A^*-模为

$$M_n^* = A^*Q_n = M_0 \oplus \cdots \oplus M_n \oplus \mathfrak{a} M_n \oplus \mathfrak{a}^2 M_n \oplus \cdots \oplus \mathfrak{a}^r M_n \oplus \cdots.$$

由于 Q_n 为有限生成 A-模，从而 M_n^* 是有限生成 A^*-模. 并且我们有 M 的 A^*-子模升链：

$$M_0^* \subseteq M_1^* \subseteq \cdots \subseteq M_n^* \subseteq \cdots \subseteq M^* = \bigcup_{n\geq 0} M_n^*.$$

由引理 1 的系知 A^* 是 Noether 环，从而不难看出：

M^*为有限生成 A^*-模

$\Longleftrightarrow$上面的升链$\{M_n^*\}$是稳定的(这里的稳定是指：存在 n_0 使得 $M^* = M_{n_0}^*$)

$\Longleftrightarrow$存在 n_0，使得对每个 $r \geq 0$ 均有 $M_{n_0+r} = \mathfrak{a}^r M_{n_0}$

$\Longleftrightarrow\{M_n\}$为稳定的 $\mathfrak{a}$-链. ▌

下一个引理和它的系是相当重要的.

引理 3 (Artin-Rees 引理) 设 A 为 Noether 环而 $\mathfrak{a}$ 是 A 的理想，M 为有限生成 A-模，M' 为 M 的 A-子模. 如果 $\{M_n\}$

是 M 之稳定的子模 $\mathfrak{a}$-链，则$\{M'\cap M_n|n\geqslant 0\}$为 M' 之稳定的子模 $\mathfrak{a}$-链.

证明 由于$\mathfrak{a}(M'\cap M_n)\subseteq M'\cap \mathfrak{a}M_n\subseteq M'\cap M_{n+1}$，可知$\{M'\cap M_n\}$是 $\mathfrak{a}$-链. 从而$\bigoplus\limits_{n=0}^{\infty}(M'\cap M_n)$是分次 A^*-模，并且它是 M^* 的 A^*-子模. 由于 A 是 Noether 环，从而 A^* 是 Noether 环(引理 1 的系). 于是由 $\mathfrak{a}$-链$\{M_n\}$ 的稳定性可知 M^* 为 Noether A^*-模（引理 2），从而其子模$\bigoplus\limits_{n=0}^{\infty}(M'\cap M_n)$ 也是 Noether A^*-模. 再由引理 2 即知$\{M'\cap M_n\}$为稳定的 $\mathfrak{a}$-链. ▌

取 $M_n=\mathfrak{a}^nM$ 我们便得到

系 $A,\mathfrak{a},M$ 和 M' 如引理 3 所述. 则存在 $k\geqslant 0$，使得对每个 $n\geqslant k$ 均有$(\mathfrak{a}^nM)\cap M'=\mathfrak{a}^{n-k}(\mathfrak{a}^kM\cap M')$. ▌

引理 4 设 A 为 Noether 环，$\mathfrak{a}$ 为 A 的理想. 则

(1) $G_{\mathfrak{a}}(A)=\bigoplus\limits_{n=0}^{\infty}\mathfrak{a}^n/\mathfrak{a}^{n+1}$ 为 Noether环.

(2) 如果 M 是有限生成 A-模，$\{M_n\}$为 M 之稳定的子模 $\mathfrak{a}$-链，则$G_{\mathfrak{a}}(M)=\bigoplus\limits_{n=0}^{\infty}M_n/M_{n+1}$ 是分次的 Noether $G_{\mathfrak{a}}(A)$-模.

证明 (1) 设 $\mathfrak{a}=Au_1+\cdots+Au_s$. 以 $\bar{u}_i$ 表示 u_i 在 $\mathfrak{a}/\mathfrak{a}^2$ 中的象.不难看出，作为 $A/\mathfrak{a}$-代数，$G_{\mathfrak{a}}(A)$是由 $\bar{u}_1,\cdots,\bar{u}_s$ 生成的. 由于 A 的商环 $A/\mathfrak{a}$ 也是 Noether 环. 从而 $G_{\mathfrak{a}}(A)$ 为 Noether 环(引理 1).

(2) 由引理条件可知存在 n_0，使得对每个 $r\geqslant 0$ 均有$M_{n_0+r}=\mathfrak{a}^rM_{n_0}$. 于是 $G_{\mathfrak{a}}(M)$ 是由$\bigoplus\limits_{n\leqslant n_0}G_n(M)$生成的 $G_{\mathfrak{a}}(A)$-模，其中 $G_n(M)=M_n/M_{n+1}$ 均是 Noether A-模. 从而$\bigoplus\limits_{n\leqslant n_0}G_n(M)$ 是有限生成 $A/\mathfrak{a}$-模. 所以 $G_{\mathfrak{a}}(M)$ 是有限生成 $G_{\mathfrak{a}}(A)$-模. 由于 $G_{\mathfrak{a}}(A)$是 Noether 环，从而 $G_{\mathfrak{a}}(M)$是 Noether $G_{\mathfrak{a}}(A)$-模. ▌

下面介绍分次模的 Hilbert 多项式.

定义 设$A=\bigoplus_{n=0}^{\infty} A_n$是分次环,$M=\bigoplus_{n=0}^{\infty} M_n$和$N=\bigoplus_{n=0}^{\infty} N_n$均为分次$A$-模. A-模同态$f:M\to N$叫作是**分次的**,是指存在$k\in\mathbf{Z}$,使得对每个$n\geqslant 0$均有$f(M_n)\subseteq N_{n+k}$(如果$m<0$,我们规定$N_m=(0)$),而这时k叫作分次同态f的**次数**.

A的理想$\mathfrak{a}$叫作是**齐次的**,是指它满足以下条件:若$x\in\mathfrak{a}$,则x的所有齐次分量均属于$\mathfrak{a}$. 类似地定义一个分次A-模N的子模N'叫作是齐次的,是指:如果$x\in N'$,则x的所有齐次分量均属于N'.

分次同态$f:M\to N$的核必然是M的齐次子模. 事实上,如果$a=(a_0,a_1,\cdots,a_n,\cdots)\in \operatorname{Ker} f$,则$f(a)=(b_0,b_1,\cdots,b_n,\cdots)=0$. 其中$b_{n+k}=f(a_n)$,这里$k$为齐次同态$f$的次数. 于是$f(a_n)=b_{n+k}=0$,即$a_n\in\operatorname{Ker} f$ $(n\geqslant 0)$. 这就表明$\operatorname{Ker} f$是M的齐次子模. 同样地,$\operatorname{Im} f$也是N的齐次子模. 由于f在子模M_n上的限制$f_n:M_n\to N_{n+k}$是A_0-模同态. 若令$K_n=\operatorname{Ker} f_n$, $I_n=\operatorname{Im} f_{n-k}$,则$\operatorname{Ker} f=\bigoplus_{n\geqslant 0} K_n$, $\operatorname{Im} f=\bigoplus_{n\geqslant k} I_n$.

本节以下我们假定

(I) 分次环$A=\bigoplus_{n\geqslant 0} A_n$为 Noether 环,并且$A_0$是 Artin 环(从而也是 Noether 环).

(II) M为有限生成分次A-模,$M=\bigoplus_{n\geqslant 0} M_n$.

在这些假定之下,每个M_n均是有限生成A_0-模. 这是因为:可以象引理 1 的证明中那样令$A_+=Au_1+\cdots+Au_s$,其中$u_1,\cdots,u_s$为A中齐次元素,并且$\deg u_i=k_i\geqslant 1$. 在引理 1 中证明了$A==A_0[u_1,\cdots,u_s]$. 同样地,有限生成A-模M的一组生成元$y_1,\cdots,y_l$也可取成为M中的齐次元素. 令$\deg y_i=h_i(1\leqslant i\leqslant l)$. 于是$M_n$中元素$x$均可表示成$x=\sum_{i=1}^{l}a_iy_i$, $a_i\in A=A_0[u_1,\cdots,$

$u_s]$. 由于 $\sum_{i=1}^{t} a_i y_i$ 的 n 次分量也等于 x，从而每个 a_i 可以只用它的 $n-h_i$ 次的分量. 换句话说，我们不妨假定 a_i 是 $n-h_i$ 次齐次元素. 但是 $A=A_0[u_1,\cdots,u_s]$中的 λ 次齐次元素都是单项式 $u_1^{\alpha_1}\cdots u_s^{\alpha_s}$ $(\sum_{i=1}^{s} \alpha_i k_i=\lambda)$的 A_0-线性组合，而这样的单项式只有有限多个. 从而每个 M_n 均是有限生成 A_0-模.

由于 A_0 是 Artin 环. 因此 M_n 既是 Artin A_0-模，又是 Noether A_0-模. 因此 A_0-模 M_n 有合成列. 我们以 $l(M_n)$ 表示 M_n 的合成列长度.

定义 $P(M,t)=\sum_{n=0}^{\infty} l(M_n)t^n \in \mathbf{Z}[[t]]$叫作是分次 A-模 M 的 Poincaré 级数.

定理 1 (Hilbert-Serre) 设 $A=\bigoplus_{n\geq 0} A_n$ 和 $M=\bigoplus_{n\geq 0} M_n$ 满足上述假定(I)和(II). 如果 A 作为 A_0-代数可由齐次元素 $u_1,\cdots,u_s$ 生成，$\deg u_i=k_i\geq 1(1\leq i\leq s)$，则

$$P(M,\ t)=f(t)/\prod_{i=1}^{s}(1-t^{k_i}),\text{其中 } f(t)\in \mathbf{Z}[t](\text{多项式}).$$

证明 我们对 s 归纳. 如果 $s=0$，则 $A=A_0$. 于是 M 为有限生成 A_0-模. 从而对充分大的 n 必然 $M_n=0$. 即 $P(M,t)\in \mathbf{Z}[t]$. 取 $f(t)=P(M,t)$可知定理 1 对于 $s=0$ 成立.现在设 $s\geq 1$，考虑 M 的 A-模同态

$$\varphi: M\to M,\quad x\mapsto u_s x \quad (x\in M).$$

这是 k_s 次的分次同态. 从而 Ker φ 和 Im φ 均为 M 的齐次子模. 于是 $\text{Ker}\,\varphi=\bigoplus_{n\geq 0} K_n$，$C=M/\text{Im}\varphi=\bigoplus_{n\geq 0} C_n$. 令 φ 在 M_n 上的限制

为$\varphi_n: M_n \to M_{n+k_s}$,则$K_n = \mathrm{Ker}\,\varphi_n$, $C_{n+k_s} = M_{n+k_s}/\mathrm{Im}\,\varphi_n$. 从而有$A_0$-模正合序列

$$0 \to K_n \xrightarrow{i} M_n \xrightarrow{\varphi_n} M_{n+k_s} \xrightarrow{p} C_{n+k_s} \to 0\ .$$

于是我们有$l(M_n) - l(M_{n+k_s}) = l(K_n) - l(C_{n+k_s})$. 将此式乘以$t^{n+k_s}$,然后对$n=0,1,2,\cdots$的诸等式相加,便得到

$$(*)\quad (t^{k_s}-1)P(M,t) = P(K,t)t^{k_s} - P(C,t) + g(t),$$
$$g(t) \in \mathbf{Z}[t].$$

由于$u_sK=(0)$,$u_sC=(0)$, 从而K和C均可看成是A/u_sA-模. 而A/u_sA为分次环. 作为$A_0/u_sA \cap A_0 = A_0$上的代数,A/u_sA是由$\bar{u}_1, \cdots, \bar{u}_{s-1}$生成的,并且$\deg \bar{u}_i = k_i (1 \leqslant i \leqslant s-1)$. 从而由归纳假设我们有

$$P(K,t) = f_1(t)\Big/\prod_{i=1}^{s-1}(1-t^{k_i}), P(C,t) = f_2(t)\Big/\prod_{i=1}^{s-1}(1-t^{k_i}),$$
$$f_1(t), f_2(t) \in \mathbf{Z}[t].$$

将它们代入(*)式,即知$P(M,t) = f(t)\Big/\prod\limits_{i=1}^{s}(1-t^{k_i})$,其中$f(t)$

$$= -t^{k_s}f_1(t) + f_2(t) - g(t)\prod_{i=1}^{s-1}(1-t^{k_i}) \in \mathbf{Z}[t]. \ \blacksquare$$

一个重要情形是$u_i(1 \leqslant i \leqslant s)$均为一次齐次元素的时候. 例如对多项式环$A = A_0[x_1, \cdots, x_s]$($A_0$为Artin环)就是这种情形. 这时,对每个有限生成分次A-模,则有

$$P(M,t) = f(t)/(1-t)^s, f(t) \in \mathbf{Z}[t].$$

定理 2(Hilbert-Serre) 设A和M满足假定(I)和(II), 并且作为A_0-代数,A是由一次齐次元素$u_1, \cdots, u_s$生成的. 则存在唯一多项式$H(M,t) \in \mathbf{Q}[t]$,$\deg H(M,t) \leqslant s-1$, 使得对每个充分大的$n$均有$l(M_n) = H(M,n)$.

证明 对于$P(M, t) = \sum\limits_{n=0}^{\infty} l(M_n)t^n = f(t)/(1-t)^s$中的多

项式 $f(t)\in \mathbf{Z}[t]$,用 $(1-t)^s$ 去除，则得到唯一的 $q(t)$，$r(t)\in \mathbf{Z}[t]$,$\deg r(t)\leqslant s-1$，使得 $f(t)=(1-t)^s q(t)+r(t)$. 将 $r(t)$ 按 $(1-t)$ 展开则有

$$r(t)=a_0+a_1(1-t)+\cdots+a_{s-1}(1-t)^{s-1},a_i\in \mathbf{Q}.$$

于是

$$(*)\quad P(M,t)=q(t)+\frac{a_0}{(1-t)^s}+\cdots+\frac{a_{s-1}}{1-t}.$$

但是根据初等代数，

$$\frac{1}{(1-t)^k}=\frac{1}{(k-1)!}\sum_{n=0}^{\infty}(n+1)(n+2)\cdots(n+k-1)t^n.$$

此式左边 t^n 的系数是 n 的 $k-1$ 次多项式，并且系数均是有理数. 所以取 $\frac{a_0}{(1-t)^s}+\cdots+\frac{a_{s-1}}{1-t}$ 中 t^n 的系数为 $H(M,n)$，则 $H(M,t)\in \mathbf{Q}[t]$. $\deg H(M,t)\leqslant s-1$. 并且由 $(*)$ 式可知当 $n>\deg q(t)$ 时，$H(M,n)=l(M_n)$.

最后，当 $n>\deg q(t)$ 时，$H(M,t)$ 是次数 $\leqslant s-1$ 的多项式，并且它在 $t=n$，$n+1$，$\cdots$，$n+s-1$ 处的值为整数 $l(M_n)$，$l(M_{n+1}),\cdots,l(M_{n+s-1})$. 这就唯一地决定了多项式 $H(M,t)$. ▌

定义 定理 2 中的多项式 $H(M,t)$ 叫作是分次 A-模的 **Hilbert 多项式**.

从定理 2 的证明可知 $H(M,t)$ 有形式

$$H(M,t)=\sum_{k=0}^{s-1}a_i'\binom{t+k}{k},a_i'\in \mathbf{Z},\ \binom{t}{k}=\frac{t(t-1)\cdots(t-k+1)}{k!}.$$

注意对于充分大的整数 n，$H(M,n)$ 均为整值. 由这一事实也可推出 $H(M,t)$ 有上述形式.

例 最简单例子为 $A=M=k[x_1,\cdots,x_s]$，其中 k 为域. 而 $A_n=M_n=n$ 次齐次多项式全体. A 作为 $A_0=k$ 上的代数是由一次齐次元素 $x_1,\cdots,x_s$ 生成的. 而 M_n 作为 k 上向量空间以 $\{x_1^{\alpha_1}$

$\cdots x_s^{\alpha_s} | \alpha_1 + \cdots + \alpha_s = n\}$为基. 于是$l(M_n) = \dim_k M_n = \binom{n+s-1}{s-1}$（这是$n$的$s-1$次多项式）. 从而

$$P(M, t) = \sum_{n=0}^{\infty} \binom{n+s-1}{s-1} t^n = 1/(1-t)^s, H(M, t) = \binom{t+s-1}{s-1}.$$

记号 设A和M满足上述条件(I)和(II). $P(M, t)$是分次A-模M的 Poincaré 级数. 我们以$\tilde{d}(M)$表示$P(M, t)$在$t=1$处的极点阶数. 比如上例中$A = M = k[x_1, \cdots, x_s]$,则$\tilde{d}(M) = s$.

我们知道,在定理 2 的假定下,Hilbert 多项式$H(M, t)$的次数不超过$s-1$. 现在我们可以求出它的确切次数.

引理 5 在定理2的假定下,我们有$\deg H(M, t) = \tilde{d}(M) - 1$.

证明 根据定理 2 证明中的(*)式和$\tilde{d}(M)$的定义,可知

$$P(M, t) = q(t) + \frac{a_{s-\tilde{d}(M)}}{(1-t)^{\tilde{d}(M)}} + \cdots + \frac{a_{s-1}}{1-t}, \quad a_{s-\tilde{d}(M)} \neq 0$$

而右边展成形式幂级数后,t^n的系数是n的$\tilde{d}(M)-1$次多项式,由此即证引理. ▌

引理 6 设$(A, \mathfrak{m})$为 Noether 局部环, $\mathfrak{q}$为A的$\mathfrak{m}$-准素理想,M为有限生成A-模,$\{M_n\}$是M之稳定的子模$\mathfrak{q}$-链. 则

(1) 对于每个$n \geqslant 0$,A-模M/M_n的长度有限.

(2) 令s为理想$\mathfrak{q}$的生成元最少个数,则存在多项式$g(t) \in \mathbb{Q}[t]$,$\deg g(t) \leqslant s$,使得对充分大的n均有$l(M/M_n) = g(n)$.

(3) $\deg g(t)$和$g(t)$的首项系数只依赖于M和$\mathfrak{q}$而与$\{M_n\}$的选取无关.

证明 (1) 考虑$G(A) = \bigoplus_{n \geqslant 0} \mathfrak{q}^n/\mathfrak{q}^{n+1}$和$G(M) = \bigoplus_{n \geqslant 0} M_n/M_{n+1}$,则$G_0(A) = A/\mathfrak{q}$为 Artin 局部环,$G(A)$为 Noether 环, $G(M)$为 Noether 分次$G(A)$-模(引理 4). 由题设知M为 Noether A-模,

从而 M_n/M_{n+1} 均是有限生成 A-模. 由于 $\mathfrak{q}(M_n/M_{n+1})=(0)$，从而 M_n/M_{n+1} 也是有限生成 $A/\mathfrak{q}$-模. 但是 $A/\mathfrak{q}$ 为 Artin 环，所以 M_n/M_{n+1} 作为 $A/\mathfrak{q}$-模，或者同样地作为A-模，既是 Noether 模又是 Artin 模. 于是其合成列长度 $l(M_n/M_{n+1})$有限. 从而

$$l(M/M_n)=\sum_{r=1}^{n} l(M_{r-1}/M_r) \qquad (*)$$

也有限，即 M/M_n之合成列长度 $l_n=l(M/M_n)$有限.

(2) 如果 $u_1,\cdots,u_s$ 生成$\mathfrak{q}$，则作为 $A/\mathfrak{q}$-代数，$G(A)$ 是由$\mathfrak{q}/\mathfrak{q}^2$ 中元素 $\bar{u}_1,\cdots,\bar{u}_s$ 生成的，而 $\deg \bar{u}_i=1(1\leqslant i\leqslant s)$.因为 $A/\mathfrak{q}$ 为 Artin 环，利用定理 2 即知对充分大的 n 均有 $l(M_n/M_{n+1})=H(G(M),n)$，其中 $H(G(M),t)$是 $G(M)$的 Hilbert 多项式，次数$\leqslant s-1$. 于是由($*$)式可知 $l_{n+1}-l_n=H(G(M),n)$. 由此可知存在一个多项式 $g(t)\in \mathbf{Q}[t]$，$\deg g(t)=\deg H(G(M),t)+1\leqslant s$，使得对每个充分大的$n$ 均有 $l_n=l(M/M_n)=g(n)$.

(3) 设$\{\tilde{M}_n\}$是M的另一个稳定的子模 $\mathfrak{q}$-链. 令 $\tilde{g}(t)$为相应的多项式，使得对充分大的 n 均有 $l(M/\tilde{M}_n)=\tilde{g}(n)$. 由于$\{M_n\}$和$\{\tilde{M}_n\}$均是稳定的 $\mathfrak{q}$-链，于是存在 n_0，使得对每个 n 均有(注意 $M_0=\tilde{M}_0=M$)

$$\mathfrak{q}^n M\supseteq M_{n+n_0}=\mathfrak{q}^n M_{n_0}\supseteq \mathfrak{q}^{n+n_0}M, \mathfrak{q}^n M\supseteq \tilde{M}_{n+n_0}= \mathfrak{q}^n\tilde{M}_{n_0}\supseteq \mathfrak{q}^{n+n_0}M.$$

于是对每个 $n\geqslant 0$ 均有

$$M_{n+n_0}\supseteq \mathfrak{q}^{n+n_0}M\supseteq \tilde{M}_{n+2n_0}, \tilde{M}_{n+n_0}\supseteq M_{n+2n_0}.$$

于是对充分大的n 均有 $g(n+n_0)\leqslant \tilde{g}(n+2n_0)$，$\tilde{g}(n+n_0)\leqslant g(n+2n_0)$. 由此易知 $g(t)$和 $\tilde{g}(t)$有相同的次数和首项系数. ▌

定义 对于M之稳定的子模 $\mathfrak{q}$-链$\{M_n\}$，$M_n=\mathfrak{q}^n M$，由引理 6 中给出的多项式 $g(t)$表示成 $\chi_{\mathfrak{q}}^M(t)$. 于是，对于充分大的 n 均有 $l(M/\mathfrak{q}^n M)=\chi_{\mathfrak{q}}^M(n)$.

又若取 $M=A$，则$\chi_{\mathfrak{q}}^A(t)$叫作是 Noether 局部环$(A,\mathfrak{m})$中 $\mathfrak{m}$-

准素理想 $\mathfrak{q}$ 的**特征多项式**，简记成 $\chi_{\mathfrak{q}}(t)$. 于是由引理 6 我们知道

引理 7 设$(A,\mathfrak{m})$为 Noether 局部环，$\mathfrak{q}$ 为 $\mathfrak{m}$-准素理想，s为 $\mathfrak{q}$ 之生成元最少个数. 则 $\deg\chi_{\mathfrak{q}}(t)\leqslant s$，并且对充分大的 n 均有 $l(A/\mathfrak{q}^n)=\chi_{\mathfrak{q}}(n)$. ▌

引理 8 $A,\mathfrak{m},\mathfrak{q}$ 同引理 7. 又若 $\mathfrak{q}'$也为 $\mathfrak{m}$-准素理想，则 $\deg\chi_{\mathfrak{q}}(t)=\deg\chi_{\mathfrak{q}'}(t)$.

证明 只需证明 $\deg\chi_{\mathfrak{q}}(t)=\deg\chi_{\mathfrak{m}}(t)$即可. 由于 A 为Noether 局部环，于是有 r 使得 $\mathfrak{m}\supseteq\mathfrak{q}\supseteq\mathfrak{m}^r$. 从而 $\mathfrak{m}^n\supseteq\mathfrak{q}^n\supseteq\mathfrak{m}^{nr}$. 所以对充分大的 n 均有 $\chi_{\mathfrak{m}}(n)\leqslant\chi_{\mathfrak{q}}(n)\leqslant\chi_{\mathfrak{m}}(rn)$. 令 $n\to+\infty$ 即知 $\deg\chi_{\mathfrak{q}}(t)=\deg\chi_{\mathfrak{m}}(t)$. ▌

定义 根据引理 8，对于所有的 $\mathfrak{m}$-准素理想 $\mathfrak{q}$，$\chi_{\mathfrak{q}}(t)$有相同的次数. 我们把这个共同的次数表示成$d(A)$. (A 为 Noether 局部环). 由引理 6 的证明不难看出(取$\mathfrak{q}=\mathfrak{m}$)，$d(A)$ 比 $G_{\mathfrak{m}}(A)$的 Hilbert多项式 $H(G_{\mathfrak{m}}(A),t)$的次数大 1，于是$d(A)=\tilde{d}(G_{\mathfrak{m}}(A))$，这里 $\tilde{d}(G_{\mathfrak{m}}(A))$ 是早先定义的 $G_{\mathfrak{m}}(A)=\bigoplus\limits_{n\geqslant0}\mathfrak{m}^n/\mathfrak{m}^{n+1}$的Poincaré 级数 $P(G_{\mathfrak{m}}(A),t)$在 $t=1$ 处极点阶数.

习　　题

1. 设 k 为域. (1) 对于例 2 中的分次环 $A=k[x^2,x^3]$，计算A的 Poincaré 级数 $P(A,t)$. (2) 对于A的极大理想 $\mathfrak{m}=(x^2,x^3)$，则 $\widetilde{\mathfrak{m}}=\mathfrak{m}A_{\mathfrak{m}}$为局部环$A_{\mathfrak{m}}$的唯一极大理想. 计算 $d(A_{\mathfrak{m}})$，$\chi_{\widetilde{\mathfrak{m}}}(t)$和 $\chi_{\widetilde{\mathfrak{m}}^2}(t)$.

2. k 为域，$A=k[x_1,\cdots,x_m]$，$\mathfrak{m}=(x_1,\cdots,x_m)$. 计算$d(A_{\mathfrak{m}})$.

3. 设 $A=\bigoplus\limits_{n\geqslant0}A_n$ 为分次环，$M=\bigoplus\limits_{n\geqslant0}M_n$ 为分次 A-模，S 为A的乘法集，并且S中元素均是齐次的. 令 $S_i=S\cap A_i$，

$(S^{-1}M)_i=\{m'\in S^{-1}M\mid$ 存在$j,k\geqslant0,j-k=i,m\in M_j,s\in S_k$，使得 $m'=m/s\}$.

求证 $S^{-1}A=\bigoplus\limits_{n\geqslant0}(S^{-1}A)_n$ 为分次环，而 $S^{-1}M=\bigoplus\limits_{n\geqslant0}(S^{-1}M)_n$ 为分次$S^{-1}A$-

模。并且$\varphi: M\to S^{-1}M, m\mapsto m/1$为0次的分次$A$-模同态。

4．设$A=\bigoplus\limits_{n\geq 0}A_n$为分次环，$A=A_0[A_1]$，$M=\bigoplus\limits_{n\geq 0}M_n$为分次$A$-模．$M=\sum\limits_{i\in I}Ay_i$，其中$y_i$均为$M$的齐次元素并且$\deg y_i\leqslant N(i\in I)$。求证当$n\geqslant N, k\geqslant 0$时，$M_{n+k}=A_kM_n$。

5．设$A=\bigoplus\limits_{n\geq 0}A_n$为分次环，$\mathfrak{p}=\bigoplus\limits_{n\geq 0}\mathfrak{p}_n$为$A$的齐次理想($\mathfrak{p}_n\subseteq A_n$)。求证：$\mathfrak{p}$为$A$的素理想$\Longleftrightarrow$如果$a\in A_m, b\in A_n, ab\in\mathfrak{p}$，则$a\in\mathfrak{p}$或者$b\in\mathfrak{p}$。

6．设A为Noether环，$\mathfrak{a}$和$\mathfrak{b}$为A的两个理想．求证有$h\geqslant 1$，使得$\mathfrak{a}^h\cap\mathfrak{b}\subseteq\mathfrak{ab}$。

7．设A为Noether环，$\mathfrak{a}$为A的理想，$x\in A$并且x不是A的零因子。求证有$k\geqslant 1$，使得当$n\geqslant k$时$(\mathfrak{a}^n:x)\subseteq\mathfrak{a}^{n-k}$。

以下几个习题表明分次环$A=k[x_0,x_1,\cdots,x_s]$(对于通常的分次：$A=\bigoplus\limits_{n\geq 0}A_n$，$A_n$为$A$中$n$次齐次多项式全体和零元素，$k$为任意域)与代数几何中射影代数集合的关系。

设V为k上$s+1$维向量空间．在V的全部非零向量之间定义如下的等价关系：

$(a_0,\cdots,a_s)\sim(b_0,\cdots,b_s)\Longleftrightarrow$存在$0\neq\alpha\in k$，使得$a_i=\alpha b_i(0\leqslant i\leqslant s)$。全体等价类集合叫作是$k$上$s$**维射影空间**，表示成$\mathbf{P}^s(k)$。$(a_0,\cdots,a_s)(\neq(0,\cdots,0))$所在的等价类叫作是$\mathbf{P}^s(k)$**中的点**，而$(a_0,\cdots,a_s)$叫作是此点的**齐次坐标**．于是，$\mathbf{P}^s(k)$中同一点的不同齐次坐标可相差$k$中非零常数因子。

设P为$\mathbf{P}^s(k)$中一点，$f(x_0,\cdots,x_s)\in k[x_0,\cdots,x_s]$。称$P$为$f(x_0,\cdots,x_s)$的**零点**(表示成$f(P)=0$)，是指对$P$的每个齐次坐标$(a_0,\cdots,a_s)$，$f(a_0,\cdots,a_s)=0$。

8．若k为无限域，$f(P)=0$，求证对于$f(x_0,\cdots,x_s)$的每个l次齐次成分$(l=0,1,2,\cdots)f_l$，均有$f_l(P)=0$。

9．设$\mathfrak{P}$为$\boldsymbol{P}^s(k)$的点集．求证

$I(\mathfrak{P})=\{f\in k(x_0,\cdots,x_s)|f(P)=0,对每个P\in\mathfrak{P}\}$

是$k[x_0,\cdots,x_s]$中的齐次理想．

10．设S为$k[x_0,\cdots,x_s]$中任一集合。我们称

$$V(S)=\{P\in \boldsymbol{P}^s(k)\mid f(P)=0,\text{对每个 } f\in S\}$$

为 $\boldsymbol{P}^s(k)$中射影代数集合．求证：

(1) 设 $\mathfrak{a}$ 是由 S 中所有多项式的所有齐次成分所生成的 $k[x_0,\cdots,x_s]$ 中齐次理想，则 $V(S)=V(\mathfrak{a})$.

(2) 对 $\boldsymbol{P}^s(k)$中每个射影代数集合 V，均有有限多齐次多项式 $f_1,\cdots,f_m\in k[x_0,\cdots,x_s]$，使得 $V=V(\{f_1,\cdots,f_m\})$.

(3) $\boldsymbol{P}^s(k)$中射影代数集合全体满足拓扑空间的闭集公理系统.

11．(射影空间中的 Hilbert 零点定理)．设 k 为代数封闭域，$\mathfrak{a}$ 为 $A=k[x_0,\cdots,x_s]$中的齐次理想，$A_+=\bigoplus\limits_{n\geq 1}A_n=(x_0,\cdots,x_s)$．求证

(1) $V(\mathfrak{a})=\varnothing\Longleftrightarrow$存在整数 N，使得$\mathfrak{a}\supseteq\bigoplus\limits_{n\geq N}A_n$

$$\Longleftrightarrow\sqrt{\mathfrak{a}}=A\text{ 或者 }\sqrt{\mathfrak{a}}=A_+.$$

(2) 如果 $V(\mathfrak{a})\neq\varnothing$，则 $IV(\mathfrak{a})=\sqrt{\mathfrak{a}}$.

12．$\boldsymbol{P}^s(k)$中射影代数集合 V 叫作是**可约的**，是指 $V=V_1\cup V_2$，其中 V_1 和 V_2 是比 V 小的射影代数集合．不可约射影代数集合也称作是射影代数簇，设 k 为代数封闭域，求证：

(1) $\boldsymbol{P}^s(k)$ 中射影代数集合与 A 中不等于 A_+ 的齐次根式理想一一对应.

(2) V 为 $\boldsymbol{P}^s(k)$中的射影代数簇$\Rightarrow I(V)$为 A 的齐次素理想.

(3) $\boldsymbol{P}^s(k)$ 中每个射影代数集合均可唯一地表成有限个彼此不相包含的射影代数簇之并.

§7.2 维数理论

我们已经定义过一个环 R 的 Krull 维数 $\dim R$．它是R中素理想链 $\mathfrak{p}_0\subset\mathfrak{p}_1\subset\cdots\subset\mathfrak{p}_n$ 之长度 n 的最大可能的值（当最大值不存在时令 $\dim R=+\infty$)．M. Nagata 给出了无限维 Noether 环的例子（习题 1)．但是 Noether 局部环的维数一定是有限的．更确切地说，对于 Noether 局部环$(A,\mathfrak{m})$，以 $\delta(A)$表示 A 的所有$\mathfrak{m}$-准素理想的生成元的最少个数，即

$\delta(A)=\min\{n\mid$有 A的 $\mathfrak{m}$-准素理想 $\mathfrak{q}$，$\mathfrak{q}$ 由 n 元生成$\}$，再以

$d(A)$表示$\{\chi_{\mathfrak{p}}(A) | \mathfrak{q}$ 为 $\mathfrak{m}$-准素理想$\}$的公共次数（见上节末尾），则我们有以下值得注意的结果

定理 3 设 $(A,\mathfrak{m})$ 为 Noether 局部环，则 $\delta(A)=d(A)=\dim A$.

注记 由于$\delta(A)$和$d(A)$均是有限值. 从而由此定理即知每个 Noether 局部环的 Krull 维数都是有限的.

为了证明定理 3，我们依次验证 $\delta(A)\geqslant d(A)\geqslant \dim A\geqslant \delta(A)$ 首先由引理 7 即知下面引理 9 成立.

引理 9 $\delta(A)\geqslant d(A)$. ▌

引理 10 $d(A)\geqslant \dim A$.

证明 对 $d(A)$用归纳法. 若 $d(A)=0$，则由 $d(A)$的定义可知对充分大的 n，$l(A/\mathfrak{m}^n)$ 均为常数. 从而 $\mathfrak{m}^n=\mathfrak{m}^{n+1}$. 由中山引理可知 $\mathfrak{m}^n=(0)$. 于是 A 为 Artin 环，从而 $\dim A=0$，即 $d(A)=0$ 时引理 10 成立. 现设 $d(A)\geqslant 1$，令 $\mathfrak{p}_0\subset \mathfrak{p}_1\subset\cdots\subset \mathfrak{p}_r$ 为 A 中素理想链. 取 $x\in \mathfrak{p}_1-\mathfrak{p}_0$，记 $\bar{A}=A/\mathfrak{p}_0$，这是局部整环，其唯一极大理想为$\bar{\mathfrak{m}}$. 以 $\bar{x}$ 表示 x 在 $\bar{A}$ 中的象，则 $\bar{x}\neq\bar{0}(\in\bar{A})$. 于是有 $\bar{A}$-模同构 $f:\bar{A}\to\bar{x}\bar{A}$，$y\mapsto\bar{x}y(y\in\bar{A})$.记$N=\bar{x}\bar{A}$，$N_n=N\subset\bar{\mathfrak{m}}^n\bar{A}$，则由 Artin-Rees 引理可知$\{N_n\}$为 $\bar{A}$-模N之稳定的子模 $\mathfrak{m}$-链. 并且有 $\bar{A}$-模正合序列

$$0\to N/N_n\to\bar{A}/\bar{\mathfrak{m}}^n\bar{A}\to\bar{\bar{A}}/\bar{\bar{\mathfrak{m}}}^n\bar{\bar{A}}\to 0,$$

其中$\bar{\bar{A}}=\bar{A}/\bar{x}\bar{A}$，$\bar{\bar{\mathfrak{m}}}$为$\bar{\mathfrak{m}}$在$\bar{\bar{A}}$中的象，它是$\bar{\bar{A}}$中唯一极大理想. 根据引理 6，存在多项式 $g(t)$使得对充分大 n 均有 $g(n)=l(N/N_n)$. 于是由上面正合序列可知对充分大的 n 均有 $g(n)-\chi_{\bar{\mathfrak{m}}}^{\bar{A}}(n)+\chi_{\bar{\bar{\mathfrak{m}}}}^{\bar{\bar{A}}}(n)=0$. 但是我们有 $\bar{A}$-模同构 $N\cong\bar{A}$. 从而由引理 6 知 $g(t)$与 $\chi_{\bar{\mathfrak{m}}}^{\bar{A}}(t)$有相同的次数和首项系数. 这就表明 $\deg\chi_{\bar{\bar{\mathfrak{m}}}}^{\bar{\bar{A}}}(t)\leqslant\deg\chi_{\bar{\mathfrak{m}}}^{\bar{A}}(t)-1$. 即 $d(\bar{\bar{A}})\leqslant d(\bar{A})-1$. 另一方面，由于 $\bar{A}/\bar{\mathfrak{m}}^n$是$A/\mathfrak{m}^n$ 的同态象，从而 $l(\bar{A}/\bar{\mathfrak{m}}^n)\leqslant l(A/\mathfrak{m}^n)$. 于是 $d(\bar{A})\leqslant$

$d(A)$. 从而 $d(\overline{\overline{A}})\leqslant d(A)-1$. 由此用归纳假设,可知环 $\overline{\overline{A}}$ 中素理想链的长度均不超过 $d(A)-1$. 但是$\overline{\overline{\mathfrak{p}_1}}\subset\overline{\overline{\mathfrak{p}_2}}\subset\cdots\subset\overline{\overline{\mathfrak{p}_r}}$是$\overline{\overline{A}}$中长为 $r-1$ 的素理想链. 于是 $r-1\leqslant d(A)-1$, 即 $r\leqslant d(A)$ 这就证明了 $\dim A\leqslant d(A)$. ▌

定义 设 $\mathfrak{p}$ 为环 A 的素理想,则形如 $\mathfrak{p}_0\subset\mathfrak{p}_1\subset\cdots\subset\mathfrak{p}_r=\mathfrak{p}$ 的 A 中素理想链长度 r 的最大值称作是 $\mathfrak{p}$ 的**高**,表示成 $h(\mathfrak{p})$. 由于 A 与局部环 $A_{\mathfrak{p}}$ 中素理想之间的保序对应关系, 可知 $h(\mathfrak{p})=\dim A_{\mathfrak{p}}$.

引理 11 设$(A,\mathfrak{m})$为 Noether 局部环, $d=\dim A$. 则存在 A 中一个 $\mathfrak{m}$-准素理想 $\mathfrak{q}$,它由 d 个元素 $u_1,\cdots,u_d$ 生成.于是$\dim A\geqslant\delta(A)$.

证明 不妨设 $d\geqslant 1$. 我们首先归纳构作一组元素 $u_1,\cdots,u_d$ 满足如下性质: 对于每个 $i(1\leqslant i\leqslant d)$和包含$\{u_1,\cdots,u_i\}$ 的每个素理想 $\mathfrak{p}$,均有 $h(\mathfrak{p})\geqslant i$.

设 $u_1,\cdots,u_{i-1}$ 已构作好. 以 $\mathfrak{p}_j(1\leqslant j\leqslant s)$表示属于理想$\mathfrak{a}=(u_1,\cdots,u_{i-1})$(当 $i=1$ 时, 取 $\mathfrak{a}=(0)$)的全部极小素理想之中高为 $i-1$ 的那些(如果没有这样的极小素理想则令 $s=0$). 由于$i-1<d=\dim A=h(\mathfrak{m})$,从而 $\mathfrak{m}\neq\mathfrak{p}_j(1\leqslant j\leqslant s)$. 于是 $\mathfrak{m}\not\subseteq\bigcup\limits_{j=1}^{s}\mathfrak{p}_j$.

取 $u_i\in\mathfrak{m},u_i\notin\bigcup\limits_{j=1}^{s}\mathfrak{p}_j$,设 $\mathfrak{q}$ 为包含$\{u_1,\cdots,u_i\}$的一个素理想,则 $\mathfrak{q}$ 必包含属于理想$(u_1,\cdots,u_{i-1})$的某个极小素理想 $\mathfrak{p}$. 如果 $\mathfrak{p}=\mathfrak{p}_j$ (对某个 j),则 $u_i\in\mathfrak{q},u_i\notin\mathfrak{p}$,从而 $\mathfrak{q}\supset\mathfrak{p}$. 于是 $h(\mathfrak{q})\geqslant h(\mathfrak{q})+1\geqslant i-1+1=i$. 如果 $\mathfrak{p}\neq\mathfrak{p}_j$ $(1\leqslant j\leqslant s)$, 则 $h(\mathfrak{p})\geqslant i$. 从而 $h(\mathfrak{q})\geqslant h(\mathfrak{p})\geqslant i$. 这就表明对于每个包含 $\{u_1,\cdots,u_i\}$ 的素理想 $\mathfrak{q}$, 均有 $h(\mathfrak{q})\geqslant i$.

现在按上述方法构造出 $u_1,\cdots,u_d$. 考虑理想 $\mathfrak{q}=(u_1,\cdots,$

u_d). 令 $\mathfrak{p}$ 是属于 $\mathfrak{q}$ 的素理想,则 $h(\mathfrak{p})\geqslant d$,从而必然 $\mathfrak{p}=\mathfrak{m}$. 于是属于 $\mathfrak{q}$ 的素理想只有 $\mathfrak{m}$. 这表明 $\mathfrak{q}$ 是 $\mathfrak{m}$-准素理想. 这就完成了引理 11 的证明. ▌

综合引理 9,10 和 11,我们便完全证明了定理 3. 定理 3 有许多有益的推论.

系 1 设$(A, \mathfrak{m})$为 Noether 局部环, 则 $\dim A\leqslant\dim_k(\mathfrak{m}/\mathfrak{m}^2)$,其中 $k=A/\mathfrak{m}$ 为局部环 A 的剩余类域.

证明 若 $u_1,\cdots,u_s\in\mathfrak{m}$, 使得它们在 $\mathfrak{m}/\mathfrak{m}^2$ 中的象是 k-向量空间 $\mathfrak{m}/\mathfrak{m}^2$ 的一组基, 则由第二章可知 $u_1,\cdots,u_s$ 生成 $\mathfrak{m}$. 于是 $\dim_k(\mathfrak{m}/\mathfrak{m}^2)=s\geqslant\delta(A)=\dim A$. ▌

系 2 设$(A,\mathfrak{m})$为 Noether 局部环,$x\in\mathfrak{m}$,并且 x 不是 A 的零因子,则 $\dim A/(x)=\dim A-1$.

证明 如引理 10 的证明中所显示的那样,我们可得到$\dim A/(x)=d(A/(x))\leqslant d(A)-1=\dim A-1$. 另一方面,记$d=\dim A/(x)$.注意$(A/(x),\mathfrak{m}/(x))$为 Noether 局部环,设$u_i(1\leqslant i\leqslant d)$属于 $\mathfrak{m}$,并且它们在 $A/(x)$中的象生成一个 $\mathfrak{m}/(x)$-准素理想, 则$(x, u_1,\cdots,u_d)$是 A 中的 $\mathfrak{m}$-准素理想. 从而 $d+1\geqslant d(A)=\dim A$. 这就证明了 $\dim A/(x)=\dim A-1$. ▌

例 1 设 A_0 为 Artin 环,$A=A_0[x_1,\cdots,x_s]$为多项式环, $\mathfrak{m}=(x_1,\cdots,x_s)\in\mathrm{Max}\,A$. 则分次环 $G_{\mathfrak{m}}(A_{\mathfrak{m}})$同构于 A. 于是 $G_{\mathfrak{m}}(A_{\mathfrak{m}})$的 Poincaré 级数是$(1-t)^{-s}$. 由定理 3 即知 $\dim A_{\mathfrak{m}}=s$.

定义 设$(A,\mathfrak{m})$为 Noether 局部环. 如果 $u_1,\cdots,u_d$ 生成A的某个 $\mathfrak{m}$-准素理想,$d=\dim A$,则称$\{u_1,\cdots,u_d\}$为A的一个**参数系**. 例如上例中 $x_1,\cdots,x_s$ 就是环 $A_{\mathfrak{m}}$的参数系.

引理 12 设 $u_1,\cdots,u_d$ 是 Noether 局部环$(A,\mathfrak{m})$的一个参数系, $\mathfrak{q}=(u_1,\cdots,u_d)(d=\dim A)$是此参数系生成的 $\mathfrak{m}$-准素理想.如果 $f(t_1,\cdots,t_d)$为多项式环 $A[t_1,\cdots,t_d]$中的 s 次齐次多项

式，并且 $f(u_1,\cdots,u_d)\in\mathfrak{q}^{s+1}$，则 f 的所有系数均属于 $\mathfrak{m}$.

证明 存在着唯一的环同态 $\alpha:(A/\mathfrak{q})[t_1,\cdots,t_d]\to G_{\mathfrak{q}}(A)$，使得 $\alpha(t_i)=\bar{u}_i\in\mathfrak{q}/\mathfrak{q}^2\subseteq G_{\mathfrak{q}}(A)$，并且 α 在 $A/\mathfrak{q}$ 上的限制为恒等映射. 由于 $\mathfrak{q}=(u_1,\cdots,u_d)$，从而 α 是环的满同态. 将 $f(t_1,\cdots,t_d)$ 的系数模 $\mathfrak{q}$ 之后变成 $(A/\mathfrak{q})[t_1,\cdots,t_d]$ 中的多项式，记为 $\bar{f}(t_1,\cdots,t_d)$. 由于引理假设条件可知 $\bar{f}(\bar{u}_1,\cdots,\bar{u}_d)=\bar{0}\in\mathfrak{q}^s/\mathfrak{q}^{s+1}\subseteq G_{\mathfrak{q}}(A)$. 因此，$\bar{f}(t_1,\cdots,t_d)\in\operatorname{Ker}\alpha$，从而环 $G_{\mathfrak{q}}(A)$ 是 $(A/\mathfrak{q})[t_1,\cdots,t_d]/(\bar{f}(t_1,\cdots,t_d))$ 的同态象. 如果 $f(t_1,\cdots,t_d)$ 的系数不全属于 $\mathfrak{m}$，则 $\bar{f}(t_1,\cdots,t_d)$ 不是环 $(A/\mathfrak{q})[t_1,\cdots,t_d]$ 中的零因子. 于是

$$
\begin{aligned}
\tilde{d}(G_{\mathfrak{q}}(A)) &\leqslant \tilde{d}((A/\mathfrak{q})[t_1,\cdots,t_d]/(\bar{f}(t_1,\cdots,t_d)))\\
&\leqslant \tilde{d}((A/\mathfrak{q})[t_1,\cdots,t_d])-1 \quad \text{（习题 2）}\\
&= d-1 \quad \text{（由于 } A/\mathfrak{q} \text{ 是 Artin 环）}.
\end{aligned}
$$

这就与 $\tilde{d}(G_{\mathfrak{q}}(A))=d$ 相矛盾. 从而 f 的所有系数均属于 $\mathfrak{m}$. ▎

引理 13 设 $(A,\mathfrak{m})$ 为 Noether 局部环，$k=A/\mathfrak{m}$，$u_1,\cdots,u_d$ 为 A 的一个参数系，K 为 A 中一个子域同构于 k. 则 $u_1,\cdots,u_d$ 在 K 上代数无关.

证明 用反证法. 如果存在非零多项式 $f(t_1,\cdots,t_d)\in K[t_1,\cdots,t_d]$，使得 $f(u_1,\cdots,u_d)=0$. 记 $f=f_s+f_{s+1}+\cdots$，其中 $f_s\neq0$ 为 f 的 s 次齐次分量. 则 $f_s(u_1,\cdots,u_d)=-f_{s+1}(u_1,\cdots,u_d)+\cdots\in\mathfrak{q}^{s+1}$，其中 $\mathfrak{q}=(u_1,\cdots u_s)$ 是 $\mathfrak{m}$-准素理想. 由引理 12 可知 f_s 的系数均属于 $\mathfrak{m}$. 但是 f_s 的系数均属于 K，而又有域同构 $K\cong A/\mathfrak{m}$，从而必然 f_s 恒为 0，这就与 $f_s\neq0$ 相矛盾. ▎

定理 4 设 $(A,\mathfrak{m})$ 为 Noether 局部环，$d=\dim A$，$k=A/\mathfrak{m}$. 则下面三条件彼此等价：

(1) $G_{\mathfrak{m}}(A)$ 作为分次环同构于多项式环 $k[t_1,\cdots,t_d]$；

(2) $\dim_k(\mathfrak{m}/\mathfrak{m}^2)=d$；

(3) $\mathfrak{m}$ 可由 d 个元素生成.

证明 (1) ⇒(2)：令 $M=(t_1,\cdots,t_d)$ 为 $k[t_1,\cdots,t_d]$ 的极大理想，则 $\mathfrak{m}/\mathfrak{m}^2\cong M/M^2$（$k$-向量空间同构）. 从而 $\dim_k(\mathfrak{m}/\mathfrak{m}^2)=\dim_k(M/M^2)=d$.

(2)⇒(3)：设 $u_1,\cdots,u_d\in\mathfrak{m}$，使得 $\mathfrak{m}/\mathfrak{m}^2=ku_1+\cdots+ku_d$，则 $u_1,\cdots,u_d$ 生成 $\mathfrak{m}$.

(3)⇒(1)：设 $\mathfrak{m}=(u_1,\cdots,u_d)$，在引理 12 的证明中取 $\mathfrak{q}=\mathfrak{m}$，可知那里的同态 $\alpha: k[t_1,\cdots,t_d]\to G_{\mathfrak{m}}(A)$ 事实上为分次环的同构（即 $\operatorname{Ker}\alpha=(0)$）. ▌

定义 满足定理 4 条件的 Noether 局部环 A 叫作是**正则**的.

例 2 设 k 为代数封闭域，$A=k[x_1,\cdots,x_d]$，$\mathfrak{m}=(x_1,\cdots,x_d)$. 则 Noether 局部环 $A_{\mathfrak{m}}$ 为仿射空间 k^d 在原点 $(0,\cdots,0)$ 处的局部环. 令 $\overline{\mathfrak{m}}=\mathfrak{m}A_{\mathfrak{m}}$，则 $\overline{\mathfrak{m}}/\overline{\mathfrak{m}}^2\cong\mathfrak{m}/\mathfrak{m}^2$. 由此 $G_{\overline{\mathfrak{m}}}(A_{\mathfrak{m}})$ 作为分次环同构于多项式环 $k[t_1,\cdots,t_d]$（元素 $\bar{x}_i\in\overline{\mathfrak{m}}/\overline{\mathfrak{m}}^2\subseteq G_{\overline{\mathfrak{m}}}(A_{\mathfrak{m}})$ 对应于 t_i），而 $\dim A_{\mathfrak{m}}=d$（例 1）. 从而由定理 4 可知 $A_{\mathfrak{m}}$ 为正则 Noether 局部环.

最后我们谈谈 Noether 局部环的维数理论在代数几何中的应用. 首先是 Noether 环的一个结果.

引理 14 设 A 为 Noether 环，$u_1,\cdots,u_r\in A$. 则对于属于理想 $(u_1,\cdots,u_r)$ 的每个极小素理想 $\mathfrak{p}$，均有 $h(\mathfrak{p})\leqslant r$.

证明 $(A_{\mathfrak{p}},\mathfrak{p}A_{\mathfrak{p}})$ 为 Noether 局部环，而 $(u_1,\cdots,u_r)$ 在 $A_{\mathfrak{p}}$ 中的扩张理想为 $\mathfrak{m}$-准素理想，$\mathfrak{m}=\mathfrak{p}A_{\mathfrak{p}}$（这是因为 $\mathfrak{m}$ 为 $A_{\mathfrak{p}}$ 中包含 $(u_1,\cdots,u_r)$ 的唯一素理想）. 于是 $r\geqslant\dim A_{\mathfrak{p}}=h(\mathfrak{p})$. ▌

定理 5（Krull 主理想定理） 设 A 为 Noether 环，$x\in A-U(A)$，并且 x 不是 A 的零因子. 则对于属于理想 (x) 的每个极小素理想 $\mathfrak{p}$，均有 $h(\mathfrak{p})=1$.

证明 由引理 14 可知 $h(\mathfrak{p})\leqslant 1$. 如果 $h(\mathfrak{p})=0$，则 $\mathfrak{p}$ 是属于

(0)的极小素理想．从而$\mathfrak{p}$中元素均是零因子．这与$x\in\mathfrak{p}$并且x不为零因子的假定相矛盾．因此$h(\mathfrak{p})=1$．▌

引理 15 设k为代数封闭域，则多项式环$k[x_1,\cdots,x_m]$的Krull维数为m．

证明 由定义知$\dim k[x_1,\cdots,x_m]=\sup\{h(\mathfrak{m})\mid\mathfrak{m}\in\mathrm{Max}\, k[x_1,\cdots,x_m]\}$．但是在第六章中我们已经证明了每个极大理想均有形式$\mathfrak{m}=(x_1-a_1,\cdots,x_m-a_m)$，$a_i\in k$．在引理14中取$\mathfrak{a}=\mathfrak{p}=\mathfrak{m}$，即知$h(\mathfrak{m})\leqslant m$．另一方面，$\mathfrak{p}_i=(x_1-a_1,\cdots,x_i-a_i)$均是素理想$(1\leqslant i\leqslant m)$，而$(0)\subset\mathfrak{p}_1\subset\mathfrak{p}_2\subset\cdots\subset\mathfrak{p}_m=\mathfrak{m}$．从而$h(\mathfrak{m})\geqslant m$．于是对每个极大理想$\mathfrak{m}$均有$h(\mathfrak{m})=m$．从而$\dim k[x_1,\cdots,x_m]=m$．▌

定理 6 设k为代数封闭域．$R=k[x_1,\cdots,x_m]$，$f_i(x_1,\cdots,x_m)\in R(1\leqslant i\leqslant n)$，并且$m>n$．如果方程组$f_i(x_1,\cdots,x_m)=0(1\leqslant i\leqslant n)$在$k$中有解，则必有无穷多组解．

证明 设该方程组只有有限多解$(a_1^{(i)},\cdots,a_m^{(i)})$，$a_j^{(i)}\in k(1\leqslant i\leqslant r,r\geqslant 1)$．令$\mathfrak{a}$是由$f_1,\cdots,f_n$生成的$R$中理想．则$\mathfrak{a}$对应于$k^m$中代数集合$V(\mathfrak{a})=\{(a_1^{(i)},\cdots,a_m^{(i)})\mid 1\leqslant i\leqslant r\}$．令$\mathfrak{a}_i=(x_1-a_1^{(i)},\cdots,x_m-a_m^{(i)})$，则$V(\mathfrak{a}_i)=\{(a_1^{(i)},\cdots,a_m^{(i)})\}$．记$\mathfrak{a}'=\mathfrak{a}_1\cdots\mathfrak{a}_r$，则$V(\mathfrak{a}')=V(\mathfrak{a})$．从而$\sqrt{\mathfrak{a}}=\sqrt{\mathfrak{a}'}$．设$\mathfrak{p}$为属于$\mathfrak{a}$的一个极小素理想，则$\mathfrak{p}\supseteq\sqrt{\mathfrak{a}}=\sqrt{\mathfrak{a}'}$．于是$\mathfrak{p}\supseteq\mathfrak{a}'=\mathfrak{a}_1\cdots\mathfrak{a}_r$．从而有$i(1\leqslant i\leqslant r)$使得$\mathfrak{p}\geqslant\mathfrak{a}_i$．但是$\mathfrak{a}_i$为极大理想，从而$\mathfrak{p}=\mathfrak{a}_i$．而$h(\mathfrak{p})=h(\mathfrak{a}_i)=m$(引理15)．这表明属于$\mathfrak{a}$的每个极小理想的高度均为$m$，而$m>n$，这就与引理14矛盾．▌

系 设k为代数封闭域，$R=k[x_1,\cdots,x_m]$，$f_1,\cdots,f_n$是R中常数项为0的多项式，$m>n$．则方程组$f_i(x_1,\cdots,x_m)=0(1\leqslant i\leqslant n)$在$k$中必有无穷多组解．

证明 因为$(0,\cdots,0)$是该方程组的解，从而由定理 6 直接推出此系. ▌

设 k 为代数封闭域，V 为 k^m 中的代数簇，$\mathfrak{p}=I(V)$为对应于 V 的素理想. $k[V]$和 $k(V)$分别是 V 的坐标环和有理函数域. 我们在第六章中已经把 $k(V)$ 在 k 上的超越次数定义为代数簇 V 的维数，表示成 $\dim V$. V 上每个点 $P=(a_1,\cdots,a_m)$ 对应着$k[V]$的极大理想 $\mathfrak{m}_P$（它是 $k[x_1,\cdots,x_m]$中极大理想$(x_1-a_1,\cdots,x_m-a_m)$在 $k[V]=k[x_1,\cdots,x_m]/\mathfrak{p}$ 中的象）. 我们把 Noether 局部环 $k[V]_{\mathfrak{m}_P}$ 的维数 $\dim k[V]_{\mathfrak{m}_P}$ 叫作是代数簇 V 在点 P 的 **局部维数**. 代数簇的维数和在各点的局部维数有如下的联系.

定理 7 设 k 为代数封闭域，V 为 k^m 中的代数簇，则 V 在每点的局部维数均等于 V 的维数.

证明 由引理 13 可知，对于 $k[V]$的每个极大理想 $\mathfrak{m}$，均有 $\dim V\geqslant \dim k[V]_{\mathfrak{m}}$（在引理 13 中取 $A=k[V]_{\mathfrak{m}}$）. 为了证明 $\dim V\leqslant \dim k[V]_{\mathfrak{m}}$，我们需要两个引理. ▌

引理 16 设 $B\subseteq A$ 为环的整性扩张，A 为整环，B 为整闭整环，$\mathfrak{m}\in \operatorname{Max}A$，$\mathfrak{n}=\mathfrak{m}\cap B$. 则 $\mathfrak{n}\in \operatorname{Max}B$，并且 $\dim A_{\mathfrak{m}}=\dim B_{\mathfrak{n}}$.

证明 由§5.1 可知 $\mathfrak{n}\in \operatorname{Max}B$. 如果 $\mathfrak{m}\supset\mathfrak{q}_1\supset\cdots\supset\mathfrak{q}_d$ 为 A 中素理想链，则这些素理想与 B 的交得到 B 中的素理想链 $\mathfrak{n}\supset\mathfrak{q}_1\cap B\supset\cdots\supset\mathfrak{q}_d\cap B$. 于是 $\dim B_{\mathfrak{n}}\geqslant\dim A_{\mathfrak{m}}$. 反之，如果 $\mathfrak{n}\supset\mathfrak{p}_1\supset\cdots\supset\mathfrak{p}_d$ 是 B 中的素理想链，则由第二提升定理可知也有 A 中的素理想链 $\mathfrak{m}\supset\mathfrak{q}_1\supset\cdots\supset\mathfrak{q}_d$. 从而又有 $\dim B_{\mathfrak{n}}\leqslant\dim A_{\mathfrak{m}}$. ▌

引理 17（正规化引理） 设 k 是代数封闭域，A 为有限生成 k-代数，k 为 A 的子域. 则存在元素 $y_1,\cdots,y_r\in A$，使得 $y_1,\cdots,y_r$ 在 k 上代数无关，而 A 在 $k[y_1,\cdots,y_r]$上整.

证明 设 $A=k[u_1,\cdots,u_n]$. 不妨设 $u_1,\cdots,u_r$ 在 k 上代数无关，而 $u_{r+1},\cdots,u_n$ 在 $k[u_1,\cdots,u_r]$ 上均是代数的. 我们对 n 归纳. 如果 $n=r$，则引理自然成立. 假设 $n>r$，并且结果对于

$n-1$ 个生成元的情形成立．由于 u_n 在 $k[u_1,\cdots,u_{n-1}]$ 上代数，从而有多项式 $0\neq f(x_1,\cdots x_n)\in k[x_1,\cdots,x_n]$，使得 $f(u_1,\cdots,u_n)=0$．以 $f_m(x_1,\cdots x_n)$ 表示多项式 f 的最高次（m 次）齐次分量．由于 k 是无限域，从而存在 $\lambda_1,\cdots,\lambda_{n-1}\in k$，使得 $f_m(\lambda_1,\cdots\lambda_{n-1},1)\neq 0$．令 $u_i'=u_i-\lambda_i u_n(1\leqslant i\leqslant n-1)$，则 $f(u_1'+\lambda_1u_n,\cdots,u_{n-1}'+\lambda_{n-1}u_n,u_n)=0$．将左边看成是 u_n 的多项式，$u_1',\cdots,u_{n-1}'$ 均作为常量，则这是关于 u_n 的 m 次多项式，并且首项系数为 $f_m(\lambda_1,\cdots,\lambda_{n-1},1)$，这是 k 中非零元素．这表明 u_n 在 $k[u_1',\cdots,u_{n-1}']$ 上整．根据归纳假设，环 $A'=k[u_1',\cdots,u_{n-1}']$ 中可选取元素 $y_1,\cdots,y_r$，使得 $y_1,\cdots,y_r$ 在 k 上代数无关，并且 A' 在 $k[y_1,\cdots,y_r]$ 上整．由于 u_n 在 A' 上整，从而 u_n 也在 $k[y_1,\cdots,y_r]$ 上整．于是 $A=A'[u_n]$ 在 $k[y_1,\cdots,y_r]$ 上整．▌

注记 我们在证明中只利用了 k 是无限域这一事实．从而这个证明对于任何无限域 k 都成立．当 k 为有限域时，正规化引理仍然成立，但是要采取另外证法．

现在我们证明定理 7．根据正规化引理我们有 $k[V]$ 的子环 $B=k[x_1,\cdots,x_d]$，使得 $B\subseteq k[V]$ 为整性扩张，从而 $d=\dim V$，并且 B 是整闭整环．根据引理 16，我们只需证 $\dim V\leqslant\dim B_{\mathfrak{n}}$ 即可，其中 $\mathfrak{n}\in \mathrm{Max}B$．但是 B 的每个极大理想均有形式 $\mathfrak{n}=(x_1-a_1,\cdots,x_d-a_d)$，$a_i\in k$．于是 $\dim B_{\mathfrak{n}}=\mathrm{d}=\dim V$．这就完成了定理 7 的证明．▌

最后我们谈一下正则 Noether 局部环的代数几何背景．

定义 设 k 为代数封闭域，$f(x_1,\cdots,x_n)$ 为 $k[x_1,\cdots,x_n]$ 中不可约多项式．则代数簇（超曲面）$f(x_1,\cdots,x_n)=0$ 上的点 $P\in k^n$ 叫作是此代数簇的**正常点**，是指 $\frac{\partial f}{\partial x_i}(1\leqslant i\leqslant n)$ 在点 P 处的值不全为 0．否则，便称 P 为**奇异点**．

定理 8 k, f 如上面定义所示. 则代数簇 $f(x_1,\cdots,x_n)=0$ 上的点 P 是正常点 $\Longleftrightarrow$ 坐标环 $A=k[x_1,\cdots,x_n]/(f)$ 对于点 P 的极大理想 $\mathfrak{m}$ 的局部环 $A_{\mathfrak{m}}$ 为正则 Noether 局部环.

证明 我们有 $\dim A_{\mathfrak{m}}=\dim A=\dim(k[x_1,\cdots,x_n]/(f))=\dim(k[x_1,\cdots,x_n])-1=n-1$. 此外, 由于 $\mathfrak{m}=(x_1-a_1,\cdots,x_n-a_n)/(f)$, $\mathfrak{m}^2=\dfrac{(x_1-a_1,\cdots,x_n-a_n)^2+(f)}{(f)}$, 从而 $\mathfrak{m}/\mathfrak{m}^2\cong(x_1-a_1,\cdots,x_n-a_n)/(x_1-a_1,\cdots,x_n-a_n)^2+(f)$, 其中 $P=(a_1,\cdots,a_n)$. 从而

$$A_{\mathfrak{m}}\text{ 正则}\Longleftrightarrow\dim_k(\mathfrak{m}/\mathfrak{m}^2)=n-1\Longleftrightarrow f\notin(x_1-a_1,\cdots,x_n-a_n)^2\Longleftrightarrow\frac{\partial f}{\partial x_i}(1\leqslant i\leqslant n)\text{ 在点 }P=(a_1,\cdots,a_n)\text{ 处不全为 }0\Longleftrightarrow\text{点 }P\text{ 为超曲面 }f=0\text{ 的正常点.}$$ ▌

习　题

1. (Nagata 关于无限维 Noether 整环的例子) 设 k 为域, $A=k[x_1,x_2,\cdots,x_n,\cdots]$(可数无穷多未定元的多项式环). $m_1<m_2<\cdots$ 为正整数列, 使得对于每个 $i\geqslant2$ 均有 $m_{i+1}-m_i>m_i-m_{i-1}$. 令 $\mathfrak{p}_i=(x_{m_i+1},\cdots,x_{m_{i+1}})$, $S=A-\bigcup\limits_{i\geqslant1}\mathfrak{p}_i$. 求证

(1) $\mathfrak{p}_i\in\operatorname{Spec}A(i\geqslant1)$.

(2) S 为 A 的乘法集.

(3) $S^{-1}A$ 为 Noether 整环.

(4) $S^{-1}A$ 中素理想 $S^{-1}\mathfrak{p}_i$ 的高为 $m_{i+1}-m_i$. 于是 $\dim S^{-1}A=+\infty$.

2. 设 $A=\bigoplus\limits_{n\geqslant1}A_n$ 为分次环, 其中 A_0 为 Artin 环, $M=\bigoplus\limits_{n\geqslant0}M_n$ 为有限生成的分次 A-模. 如果 $a\in A_k$, 并且由 $am=0, m\in M$ 可推出 $m=0$. 求证 $\tilde{d}(M/aM)=\tilde{d}(M)-1$. [提示: 利用正合序列 $0\to aM_n\to M_{n+k}\to M_{n+k}/aM_n\to0$, 并参考引理 10 的证明.]

3. Noether 环中每个素理想的高均是有限的. 由此推出: Noether 环的每个素理想降链 $\mathfrak{p}_0\supseteq\mathfrak{p}_1\supseteq\cdots\supseteq\mathfrak{p}_n\supseteq\cdots$ 必是稳定的, 即存在 n, 使得 $\mathfrak{p}_n=\mathfrak{p}_{n+1}$

$= \cdots$.

4. 设 k 为域，$A=k[x^2,x^3]$，$\mathfrak{m}=(x^2,x^3)$。求证局部环 $A_{\mathfrak{m}}$ 不是正则的 Noether 局部环。

§7.3 完 备 化

设M为A-模. 对于环A的理想降链

$$\{\mathfrak{a}_n\}: \mathfrak{a}_0 \supseteq \mathfrak{a}_1 \supseteq \cdots \supseteq \mathfrak{a}_n \supseteq \cdots$$

我们可以在M中引进如下的拓扑：对于每个$x \in M$，规定$\{x+\mathfrak{a}_n M \mid n \geqslant 0\}$为$x$的基本开集组. 而任意多个形如$x+\mathfrak{a}_n M$ $(x \in M, n \geqslant 0)$的集合之并均是M中的开集. 这种开集全体形成的集族是满足拓扑空间的开集公理的，因为

(1) $M=\bigcup\limits_{x \in M}(x+\mathfrak{a}_0 M)$和$\varnothing=\bigcup\limits_{\mathfrak{a} \in \varnothing}(x+\mathfrak{a}_0 M)$均是开集；

(2) 任意多个开集的并显然仍是开集；

(3) 如果 $z \in (x+\mathfrak{a}_n M) \cap (y+\mathfrak{a}_m M)$. 令 $q=\max(n, m)$，则不难看出 $z+\mathfrak{a}_q M \subseteq (x+\mathfrak{a}_n M) \cap (y+\mathfrak{a}_m M)$. 于是

$$(x+\mathfrak{a}_n M) \cap (y+\mathfrak{a}_m M)=\bigcup_{z \in (x+\mathfrak{a}_n M) \cap (y+\mathfrak{a}_m M)}(z+\mathfrak{a}_q M).$$

由此不难看出，任意有限个开集之交仍是开集.

于是，M由此而成为拓扑空间，称作是**$\{\mathfrak{a}_n\}$-拓扑空间**. 特别取 $M=A$，则A上如此定义的拓扑叫作是**$\{\mathfrak{a}_n\}$-拓扑**.

一个重要的特例是取$\mathfrak{a}$为A的理想，而$\mathfrak{a}_n=\mathfrak{a}^n$，这时$M$或$A$对于由理想降链$\{\mathfrak{a}^n\}$决定的拓扑叫作是**$\mathfrak{a}$-adic 拓扑**.

一个群G如果又是拓扑空间，并且映射$G \times G \to G$，$(x, y) \mapsto xy$ 和 $G \to G$，$x \mapsto x^{-1}$ 均是连续的，则称G为**拓扑群**. 类似地，设A为环而M为A-模. 如果M是拓扑加法群，并且对于每个$a \in A$，映射$M \to M$，$x \mapsto ax$ 均是连续的，则称 M 为**拓扑 A-模**. 最后，如果环A是拓扑A-模，则称A为**拓扑环**.

不难验证，A-模M对于$\{\mathfrak{a}_n\}$-拓扑是拓扑A-模，于是A对于$\{\mathfrak{a}_n\}$-拓扑是拓扑环.（例如考虑映射$f: A\times A\to A,(a,b)\mapsto ab$. 对于$ab$的一个基本开集$ab+\mathfrak{a}_n A$，我们有$(a,b)$在$A\times A$中（对于积拓扑）的开集$U=(a+\mathfrak{a}_n A)\times(b+\mathfrak{a}_n A)$使得$f(U)=(a+\mathfrak{a}_n A)(b+\mathfrak{a}_n A)\subseteq ab+\mathfrak{a}_n A$. 这就表明$f$是连续的. 其他也可类似验证.）

A模M对于$\{\mathfrak{a}_n\}$-拓扑为Hausdorff空间的充要条件是$\bigcap_{n\geq 0}\mathfrak{a}_n M=(0)$. 这是因为：如果$\bigcap_{n\geq 0}\mathfrak{a}_n M=(0)$，则对于$M$中任意两个不同的元素$x$和$y$，$x-y\neq 0$，从而存在$n\geq 0$，使得$x-y\notin \mathfrak{a}_n M$. 于是$x$的开集$x+\mathfrak{a}_n M$和$y$的开集$y+\mathfrak{a}_n M$不相交. 反之，如果$0\neq z\in\bigcap_{n\geq 0}\mathfrak{a}_n M$，则0的每个开集均包含某个基本开集$\mathfrak{a}_n M$，而$z$在$\mathfrak{a}_n M$之中. 因此$\{\mathfrak{a}_n\}$-拓扑空间$M$甚至都不是$T_1$-型的，从而更不是Hausdorff空间. 特别地，环A对于$\{\mathfrak{a}_n\}$-拓扑是Hausdorff空间$\Longleftrightarrow\bigcap_{n\geq 0}\mathfrak{a}_n=(0)$. 而$M$和$A$对于$\mathfrak{a}$-adic拓扑是Hausdorff空间的充要条件分别是$\bigcap_{n\geq 0}\mathfrak{a}^n M=(0)$和$\bigcap_{n\geq 0}\mathfrak{a}^n=(0)$.

现在我们要说明，条件$\bigcap_{n\geq 0}\mathfrak{a}^n M=(0)$和$\bigcap_{n\geq 0}\mathfrak{a}^n=(0)$并不是很苛刻的（引理19的三个系）.

引理 18 设A为Noether环，$\mathfrak{a}$为A的理想，M为有限生成A-模，M'是M的A-子模. 则M'由M的$\mathfrak{a}$-adic拓扑所诱导的拓扑和M'作为A-模本身所具有的$\mathfrak{a}$-adic拓扑是一致的.

证明 对于前一种拓扑，0在M'中的基本开集为$\mathfrak{a}^n M\cap M'$ $(n\geq 0)$，而对后一种拓扑则为$\mathfrak{a}^n M'$ $(n\geq 0)$. 但是由Artin-Rees引理（引理3）的系，存在$k\geq 0$使得对每个$n\geq k$均有$(\mathfrak{a}^n M)\cap$

$M'=\mathfrak{a}^{n-k}((\mathfrak{a}^k M)\cap M')\subseteq\mathfrak{a}^{n-k}M'$. 另一方面又显然有 $\mathfrak{a}^n M'\subseteq(\mathfrak{a}^n M)\cap M'(n\geqslant 0)$. 从而这两种拓扑是一致的. ▌

引理 19(Krull) 设 A 为 Noether 环, $\mathfrak{a}$ 为 A 的理想, M 为有限生成 A-模. 则

$$\bigcap_{n>0}\mathfrak{a}^n M=\{x\in M\mid 存在\ a\in\mathfrak{a}\ 使得(1-a)x=0\}.$$

证明 如果 $a\in\mathfrak{a}$, $(1-a)x=0$, 则 $x=ax=a^2x=\cdots=a^nx=\cdots$. 由于$a^nx\in\mathfrak{a}^nx$, 从而$x\in\bigcap_{n>0}\mathfrak{a}^n M$. 反之, 令 $M'=\bigcap_{n>0}\mathfrak{a}^n M$. 由假设知$M$为 Noether A-模, 从而 M' 是有限生成的 A-子模. 由于 M' 是 0 在M中的所有邻域之交, 从而对于子模 M' 的诱导拓扑, 0 在M'中只有一个邻域 M'. 根据引理 18, 子模 M' 的诱导拓扑与 M' 本身的 $\mathfrak{a}$-adic 拓扑是一致的. 而对后一拓扑, $\mathfrak{a}M'$ 为 0 在 M' 中的邻域. 从而 $\mathfrak{a}M'=M'$. 由于 M' 是有限生成 A-模, 可知存在 $a\in\mathfrak{a}$ 使得$(1-a)M'=(0)$. 特别对每个 $x\in M'=\bigcap_{n>0}\mathfrak{a}^n M$, 均有$(1-a)x=0$. ▌

系 1 如果 A 为 Noether 整环, $\mathfrak{a}$ 为 A 的真理想, 则 $\bigcap_{n>0}\mathfrak{a}^n=(0)$.

证明 由于 $1+\mathfrak{a}$ 没有零因子, 由引理 19 即得此系. ▌

系 2 设 A 为 Noether 环, $\mathfrak{a}$ 为 A 的理想并且 $\mathfrak{a}$ 包含在 A 的大根 $r(A)$之中, M 为有限生成 A-模. 则 $\bigcap_{n>0}\mathfrak{a}^n M=(0)$. 特别地有 $\bigcap_{n>0}\mathfrak{a}^n=(0)$.

证明 由 $\mathfrak{a}\subseteq r(A)$ 可知 $1+\mathfrak{a}\subseteq U(A)$. 然后由引理 19 即得此系. ▌

系 3 设$(A,\mathfrak{m})$为 Noether 局部环, M为有限生成 A-模, 则

$\bigcap_{n>0} \mathfrak{m}^n M=(0)$. 特别地有 $\bigcap_{n>0} \mathfrak{m}^n=(0)$.

证明 因为 $\mathfrak{m}=r(A)$,从而由系 2 即得结果. ▌

设 A 为环,$\mathfrak{a}$ 为 A 的理想,M 为 A-模. 现在我们假定 $\bigcap_{n>0} \mathfrak{a}^n=(0)$, $\bigcap_{n>0} \mathfrak{a}^n M=(0)$. 从而 A 和 M 对于 $\mathfrak{a}$-adic 拓扑均是 Hausdorff 拓扑空间. 现在我们试图在 A 和 M 中引进距离从而使它们成为距离空间. 对于每个元素 $0 \neq x \in M$. 由于 $x \notin \bigcap_{n>0} \mathfrak{a}^n M=(0)$, 并且 $\mathfrak{a}^0 M=M \supseteq \mathfrak{a} M \supseteq \cdots \supseteq \mathfrak{a}^n M \supseteq \cdots$. 从而存在唯一的 $n \geqslant 0$, 使得 $x \in \mathfrak{a}^n M-\mathfrak{a}^{n+1} M$. 我们定义 $\nu(x)=n$. 此外令 $\nu(0)=\infty$. 类似地,对于每个元素 $0 \neq a \in A$, 也有唯一的 $n \geqslant 0$ 使得 $a \in \mathfrak{a}^n-\mathfrak{a}^{n+1}$. 定义 $\nu(a)=n$,而 $\nu(0)=\infty$. 不难验证我们有(对于 $a \in A$, $x, y \in M$)

$$\nu(x)=\infty \Longleftrightarrow x=0, \quad \nu(a)=\infty \Longleftrightarrow a=0,$$
$$\nu(-x)=\nu(x), \quad \nu(-a)=\nu(a),$$
$$\nu(a x) \geqslant \nu(a)+\nu(x),$$
$$\nu(x+y) \geqslant \min (\nu(x), \nu(y)),$$

这里我们规定 $\infty+n=n+\infty=\infty \cdot \infty=\infty, \infty>n$. 如果再令 $|x|=2^{-\nu(x)}$, $|a|=2^{-\nu(a)}$(规定 $2^{-\infty}=0$),则由上面诸项可得到($a \in A, x, y \in M$)

(i) $|x| \geqslant 0$, 并且 $|x|=0 \Longleftrightarrow x=0$;

(ii) $|-x|=|x|$;

(iii) $|x+y| \leqslant \max (|x|,|y|)$;

(iv) $|a x| \leqslant|a||x|$.

最后,对于 $x, y \in M$, 定义 $d(x, y)=|x-y|$, 称作是 x 和 y 的距离. 则由(i)—(iv)得到 $d(x, y)$ 满足通常的距离公理:

(I) $d(x,y)\geqslant 0$，并且 $d(x,y)=0\Longleftrightarrow x=y$.

(II) $d(x,y)=d(y,x)$.

(III) $d(x,z)\leqslant d(x,y)+d(y,z)$.

于是 M 由此而成为距离空间. 类似地在环 A 中定义距离，使 A 也成为距离空间. 还有一点值得注意的是，由(iii)可推得比(III)更强的结果

(III′) $d(x,z)\leqslant\max(d(x,y),d(y,z))$.

现在我们可以象点集拓扑(或者泛函分析)中那样讨论距离空间的完备化问题. 但是由于我们有比(III)更强的性质(III′)，使得在某些方面比通常的程序还要简单和特殊些. 按照通常的程序，首先要定义距离空间 M 中序列的收敛性，极限和 Gauchy 序列.

定义 设$\{x_n\}$为 M 中序列，$x\in M$. 称序列$\{x_n\}$收敛于 x，或者叫作 x 是序列$\{x_n\}$的极限并且表示成 $x_n\to x$ 或者 $\lim\limits_{n\to\infty} x_n=x$，是指对每个实数 $\varepsilon>0$ 均存在 $N=N(\varepsilon)$，使得当 $n\geqslant N$ 时均有 $|x-x_n|<\varepsilon$.

对于 A 也可类似定义收敛和极限概念，并且不难看出，如果 $x_n\to x, y_n\to y, a_n\to a\ (x_n,y_n,x,y\in M, a_n,a\in A)$，则 $x_n\pm y_n\to x\pm y$, $a_nx_n\to ax$. (注意：$|ax|\leqslant|a||x|$.) 最后，由 $\bigcap\limits_{n>0}a^nM=(0)$ 不难推得，如果序列$\{x_n\}$有极限，则极限是唯一的.

定义 M 中序列$\{x_n\}$叫作是 Cauchy 序列，是指对任意 $\varepsilon>0$ 均存在 $N=N(\varepsilon)$，使得当 $m,n\geqslant N$ 时均有 $|x_n-x_m|<\varepsilon$.

这是 Cauchy 序列的通常定义. 由于我们有(III′)式，使我们有下面简单判别法：

引理 20 M 中序列$\{x_n\}$为 Cauchy 序列$\Longleftrightarrow(x_{n+1}-x_n)\to 0$.

证明 由(III′)式我们知道(设 $n\geqslant m$)，

$$|x_n-x_m|=|(x_n-x_{n-1})+(x_{n-1}-x_{n-2})+\cdots+(x_{m+1}-x_m)|$$

$$\leqslant \max(|x_n - x_{n-1}|, |x_{n-1} - x_{n-2}|, \cdots, |x_{m+1} - x_m|),$$

从而

$\{x_n\}$为 Cauchy 序列$\Longleftrightarrow$对每个 $\varepsilon>0$ 均有 $N=N(\varepsilon)$使得当 $n\geqslant N$ 时$|x_{n+1}-x_n|<\varepsilon\Longleftrightarrow(x_{n+1}-x_n)\to 0$. ▌

定义 M 中级数$\sum_{n=1}^{\infty} x_n = x_1 + x_2 + \cdots + x_n + \cdots$叫作是**收敛的**，是指序列$\{s_n\}$收敛，其中 $s_n = x_1 + \cdots + x_n$. 如果 $s_n \to s \in M$，我们也记成$\sum_{n=1}^{\infty} x_n = s$.

由引理 20 可知，级数$\sum_{n=1}^{\infty} x_n$收敛$\Longleftrightarrow x_n \to 0$.

定义 拓扑空间叫作是**完备的**，是指其中每个 Cauchy 序列均有极限.

拓扑空间 $\hat{T}$叫作是拓扑空间T的**完备化**，是指T为$\hat{T}$的稠子集，并且$\hat{T}$是完备的. 熟知若T完备则$\hat{T}=T$，并且T的完备化本质上只有一个.(即T的两个不同的完备化拓扑空间是同胚的).

设 $\mathfrak{a}$ 为环 A 的理想，M 为 A-模，并且假设$\bigcap_{n>0}\mathfrak{a}^n=(0)$，$\bigcap_{n>0}\mathfrak{a}^n M=(0)$. 现在我们象点集拓扑学中那样作 $\mathfrak{a}$-adic 拓扑环 A 和拓扑 A-模 M 的完备化. 以 $C(M)$表示 M 中全部 Cauchy 序列组成的集合. 如果$\{x_n\}$和$\{y_n\}$是 M 中的 Cauchy 序列，$a\in A$，则$\{x_n\pm y_n\}$和$\{ax_n\}$也是 M中的 Cauchy 序列. 由此将 $C(M)$作成 A-模. M中以 0 为极限的Cauchy序列全体$Z(M)$是$C(M)$的A-子模、于是我们有商A-模$\hat{M}=C(M)/Z(M)$.完全类似地，我们可以定义环$C(A)$和它的理想$Z(A)$，其中$C(A)$中元素$\{a_n\}$和$\{b_n\}$相乘定义为$\{a_nb_n\}$. 从而有商环 $\hat{A}=C(A)/Z(A)$. 进而，对于$\{a_n\}\in C(A)$和$\{x_n\}\in C(M)$，易知$\{a_nx_n\}\in C(M)$. 于是可对$C(M)$赋予 $C(A)$-模结构. 如果$\{a_n\}\in C(A)$，$\{x_n\}\in Z(M)$，则$\{a_nx_n\}\in Z(M)$.于是又诱导出 $\hat{M}=C(M)/Z(M)$上自然的$C(A)$-模结构.最后，易知 $Z(A)$将$\hat{M}$零化. 从而$\hat{M}$又赋予自然的 $\hat{A}$-模结构.

作映射 $f:A\to\hat{A}$，$f(a)=\overline{\{a\}}$，其中$\{a\}$为常量序列，$\{a\}\in C(A)$，而 $\overline{\{a\}}$表示$\{a\}$在 $C(A)/Z(A)$中的象．易知 f 为环同态，且核为(0)．(即$\{a\}\in Z(A)\Longleftrightarrow a=0$．)通过 f 我们可以将 A 看作是 $\hat{A}$ 的子环．事实上，$\hat{A}$ 是 A-代数．类似地，可将 M 看作是 $\hat{M}$ 的 A-子模．并且对于 $a\in A$，a作为 A 中元素和 $\hat{A}$ 中元素对于$\hat{M}$ 的作用是一样的．

设 $\mathfrak{b}$ 为 A 的理想．令 $\hat{\mathfrak{b}}=\{\overline{\{a_n\}}\in\hat{A}\,|\,a_n\in\mathfrak{b}\}$．这是 $\hat{A}$ 的理想．另一方面，作为 A-模，$\mathfrak{b}$ 的完备化应当为 $C(\mathfrak{b})/Z(\mathfrak{b})$．不难看出这两种看法是一致的，因为作映射 $C(\mathfrak{b})\to\hat{\mathfrak{b}}$，$\{a_n\}\mapsto\overline{\{a_n\}}$，这是 A-模满同态并且核为 $Z(\mathfrak{b})$．从而 $C(\mathfrak{b})/Z(\mathfrak{b})$和$\hat{\mathfrak{b}}$ 作为 A-模是同构的．事实上它们作为 $\hat{A}$-模也是同构的．

引理 21 设 $\mathfrak{a}$ 是环 A 的理想，M 为 A-模．$\bigcap\limits_{n>0}\mathfrak{a}^n=(0)$，$\bigcap\limits_{n>0}\mathfrak{a}^nM=(0)$．则

(1) $\bigcap\limits_{n>0}\widehat{\mathfrak{a}^n}=(0)$．从而 $\hat{A}$ 对于$\{\widehat{\mathfrak{a}^n}\}$-拓扑是 Hausdorff 拓扑环．

(2) $\widehat{\mathfrak{a}^n}\cap A=\mathfrak{a}^n$．从而 A 作为 $\{\widehat{\mathfrak{a}^n}\}$-拓扑空间 $\hat{A}$ 的子空间拓扑与 A 本身的 $\mathfrak{a}$-adic 拓扑是一致的．

(3) A 在 $\hat{A}$ 中稠密．

(4) $\hat{A}$ 对于$\{\widehat{\mathfrak{a}^n}\}$-拓扑是完备的．

证明 (1) 设$\overline{\{a_n\}}\in\bigcap\limits_{m>0}\widehat{\mathfrak{a}^m}$，则对每个 $m\geqslant 0$，$\overline{\{a_n\}}\in\widehat{\mathfrak{a}^m}$于是有$N$，使得 $n\geqslant N$ 时 $a_n\in\mathfrak{a}^m$．这表明在 A 中 $a_n\to 0$．即$\overline{\{a_n\}}=$
$=0\in\hat{A}$．

(2) 设$\overline{\{a_n\}}\in\widehat{\mathfrak{a}^m}\cap A$，则有 $b_n\in\mathfrak{a}^m$ 使得$\overline{\{a_n\}}=\overline{\{b_n\}}$，也有$a\in A$，使得$\overline{\{a_n\}}=\overline{\{a\}}$，于是$\{b_n-a\}\in Z(A)$，即 $b_n\to a$．从而对充分大的 n，$b_n-a\in\mathfrak{a}^m$，于是 $a\in\mathfrak{a}^m+b_n\subseteq\mathfrak{a}^m$．即$\overline{\{a_n\}}=\overline{\{a\}}\in\mathfrak{a}^m$．这表明$\widehat{\mathfrak{a}^m}\cap A\subseteq\mathfrak{a}^m$．而$\widehat{\mathfrak{a}^m}\cap A\supseteq\mathfrak{a}^m$ 是显然的．

(3) 设$\{a_n\}\in C(A)$. 则对每个$L\geqslant 0$,均有$N\geqslant 0$,使得n, $m\geqslant N\Rightarrow a_n-a_m\in\mathfrak{a}^L$. 令$a=a_N$,则$\overline{\{a_n\}}-\overline{\{a\}}\in\widehat{\mathfrak{a}^L}$. 这表明$A$在$\hat{A}$中稠密.

(4) 设$a_i=\overline{\{a_n^{(i)}\}}(i=1,2,3,\cdots)$为$\hat{A}$中的Cauchy序列. 则对每个$L\geqslant 0$,均有$N\geqslant 0$使得$i,j\geqslant N\Rightarrow a_i-a_j\in\widehat{\mathfrak{a}^L}$. 即$\overline{\{a_n^{(i)}-a_n^{(j)}\}}\in\widehat{\mathfrak{a}^L}$. 于是对于充分大的$n$,则$a_n^{(i)}-a_n^{(j)}\in\mathfrak{a}^L$. 另一方面,$a_N$为Cauchy序列,从而对充分大的$n$和$m$,$a_n^{(N)}-a_m^{(N)}\in\mathfrak{a}^L$. 于是对充分大的$n$和$m$,$a_n^{(n)}-a_m^{(m)}=(a_n^{(n)}-a_n^{(N)})+$ $+(a_n^{(N)}-a_m^{(N)})+(a_m^{(N)}-a_m^{(m)})\in\mathfrak{a}^L$.令$b_n=a_n^{(\ )}$,则$\{b_n\}\in C(A)$,并且对每个$L>0$和充分大的$n,i$,$b_n-a_n^{(i)}\in\mathfrak{a}^L$.于是对充分大的$i$, $a_i-\overline{\{b_n\}}\in\widehat{\mathfrak{a}^L}$. 这就表明对于$\hat{A}$中的$\{\widehat{\mathfrak{a}^n}\}$-拓扑, $\overline{\{b_n\}}$是a_i $(i=1,2,\cdots)$的极限. ▌

完全类似地可证明如下结果.

引理 22 在引理21假定之下,又设M为A-模并且$\bigcap\limits_{n>0}\mathfrak{a}^nM=(0)$,则

(1) $\bigcap\limits_{n>0}\widehat{\mathfrak{a}^n}\hat{M}=(0)$. 从而$\hat{M}$对于$\{\widehat{\mathfrak{a}^n}\}$-拓扑是Hausdorff拓扑$\hat{A}$-模.

(2) $(\widehat{\mathfrak{a}^n}\hat{M})\cap M=\mathfrak{a}^nM$. 从而$M$作为$\hat{M}$之子空间拓扑与$M$本身的$\mathfrak{a}$-adic拓扑是一致的.

(3) M在$\hat{M}$中稠密.

(4) $\hat{M}$对于$\{\widehat{\mathfrak{a}^n}\}$-拓扑是完备的. ▌

根据上述两个引理,即知$\{\widehat{\mathfrak{a}^n}\}$-拓扑环$\hat{A}$和拓扑$\hat{A}$-模$\hat{M}$分别是$\mathfrak{a}$ adic拓扑环A和拓扑A-模M的完备化.

引理 23 设A为Noether环,$\mathfrak{a}$为A的理想,M为有限生成A-模,$\bigcap\limits_{n=0}^{\infty}\mathfrak{a}^n=(0)$, $\bigcap\limits_{n=0}^{\infty}\mathfrak{a}^nM=(0)$. 则$\hat{M}=\hat{A}M$.

证明 令$M=Ax_1+\cdots+Ax_r$. 对每个元素$\hat{y}\in\hat{M}$. 由于

M 在 $\hat{M}$ 中稠密，从而有 $y_n \in M$ 使得 $y_n \to \hat{y}$. 于是 $\{y_n\} \in C(M)$，即 $y_{n+1} - y_n \to 0$. 设 $y_{n+1} - y_n \in \mathfrak{a}^{s_n} M - \mathfrak{a}^{s_n+1} M$，则 $s_n \to \infty$. 由于 $\mathfrak{a}^m M = \mathfrak{a}^m x_1 + \cdots + \mathfrak{a}^m x_r$，从而 $y_{n+1} - y_n = \sum_{j=1}^{r} a_{nj} x_j, a_{nj} \in \mathfrak{a}^{s_n}$.

记 $y_1 = \sum_{j=1}^{r} b_{1j} x_j, b_{1j} \in A$，则

$$y_n = y_1 + (y_2 - y_1) + \cdots + (y_n - y_{n-1}) = \sum_{j=1}^{r} b_{nj} x_j,$$

$$\text{其中} b_{nj} = b_{1j} + a_{1j} + \cdots + a_{n-1,j}.$$

由于 $a_{nj} \in \mathfrak{a}^{s_n}$ 而 $s_n \to \infty$，从而 r 个序列 $\{b_{nj}\}$ $(1 \leqslant j \leqslant r)$ 均为 Cauchy 序列. 从而 $\lim\limits_{n\to\infty} b_{nj} = \widehat{b_j} \in \hat{A}$. 而 $\hat{y} = \lim y_n = \sum_{j=1}^{r} \hat{b}_j x_j$. 这就证明了 $\hat{M} = \hat{A} M$. ▌

系 若 A 为 Moether 环，则 $\widehat{\mathfrak{a}^n} = \hat{\mathfrak{a}}^n$. 因此 A 和 A-模 M 的 $\{\hat{\mathfrak{a}}^n\}$-拓扑即是 $\hat{\mathfrak{a}}$-adic 拓扑.

证明 将 $\mathfrak{a}^n$ 看作是 A-模，由引理 23 即知 $\widehat{\mathfrak{a}^n} = (\hat{A}\mathfrak{a}^n) = (\hat{A}\mathfrak{a})^n = \hat{\mathfrak{a}}^n$. ▌

下面我们通过利用分次环 $G_{\mathfrak{a}}(A)$ 来证明：完备化过程保持环的 Noether 性（定理 9）.

引理 24 设 A 为 Noether 环，$\mathfrak{a}$ 为 A 的理想，$\bigcap_{n>0} \mathfrak{a}^n = (0)$. $\hat{A}$ 为 $\mathfrak{a}$-adic 拓扑环 A 的完备化. 则有环同构 $G_{\mathfrak{a}}(A) \cong G_{\hat{\mathfrak{a}}}(\hat{A})$.

证明 $G_{\mathfrak{a}}(A) = \bigoplus_{n>0} A_n, A_n = \mathfrak{a}^n / \mathfrak{a}^{n+1}, G_{\hat{\mathfrak{a}}}(\hat{A}) = \bigoplus_{n>0} \hat{A}_n$，$\hat{A}_n = \hat{\mathfrak{a}}^n / \hat{\mathfrak{a}}^{n+1}$ 由 $\hat{\mathfrak{a}}$ 的定义可知 $\mathfrak{a}^n \cap \hat{\mathfrak{a}}^{n+1} = \mathfrak{a}^{n+1}$. 进而，因为 A 在 $\hat{A}$ 中稠密，对每个 $\hat{b} \in \hat{\mathfrak{a}}^n$ 均有 $b \in A$ 使得 $\hat{b} - b \in \hat{\mathfrak{a}}^{n+1}$，于是 $b \in \hat{\mathfrak{a}}^n \cap A = \mathfrak{a}^n$，这表明 $\hat{\mathfrak{a}}^n = \mathfrak{a}^n + \hat{\mathfrak{a}}^{n+1}$. 从而我们有加法群的同构

$$\hat{A}_n = \hat{\mathfrak{a}}^n / \hat{\mathfrak{a}}^{n+1} = \frac{\mathfrak{a}^n + \hat{\mathfrak{a}}^{n+1}}{\hat{\mathfrak{a}}^{n+1}} \cong \mathfrak{a}^n / \mathfrak{a}^n \cap \hat{\mathfrak{a}}^{n+1} = \mathfrak{a}^n / \mathfrak{a}^{n+1} = A_n.$$

再由 $G_{\mathfrak{a}}(A)$和 $G_{\mathfrak{a}}(\hat{A})$中的乘法定义即知这两个环是同构的. ▌

引理 25 设 $\mathfrak{a}$ 为环 A 的理想,A 对于 $\mathfrak{a}$-adic 拓扑是完备的,M 为 R-模,$\bigcap_{n>0}\mathfrak{a}^n=(0)$,$\bigcap_{n>0}\mathfrak{a}^nM=(0)$.如果$G_{\mathfrak{a}}(M)$是有限生成 $G\mathfrak{a}(A)$-模,则 M 为有限生成 A-模.

证明 设 $G_{\mathfrak{a}}(M)=G_{\mathfrak{a}}(A)\bar{x}_1+\cdots+G_{\mathfrak{a}}(A)\bar{x}_n, x_i\in\mathfrak{a}^{e_i}M-\mathfrak{a}^{e_i+1}M$,于是 $\deg\bar{x}_i=e_i$. 我们要证 $M=Ax_1+\cdots+Ax_n$.

对每个 $u_1\in M$,设 $u_1\in\mathfrak{a}^{m_1}M-\mathfrak{a}^{m_1+1}M$,$m_1\geqslant 0$,则$0\neq\bar{u}_1\in\mathfrak{a}^{m_1}M/\mathfrak{a}^{m_1+1}M$,于是有 $a_{1i}\in\mathfrak{a}^{m_1-e_i}$,使得 $\bar{u}_1=\sum_{i=1}^{n}\bar{a}_{1i}\bar{x}_i$,$\bar{a}_{1i}\in\mathfrak{a}^{m_1-e_i}/\mathfrak{a}^{m_1-e_i+1}$ $(1\leqslant i\leqslant n)$. 于是 $u_2=u_1-\sum_{i=1}^{n}a_{1i}x_i\in\mathfrak{a}^{m_1+1}M$. 又令 $u_2\in\mathfrak{a}^{m_2}M-\mathfrak{a}^{m_2+1}M$,则 $m_2>m_1$. 同样地可有 $u_2-\sum_{i=1}^{n}a_{2i}x_i\in\mathfrak{a}^{m_2+1}M$,$a_{2i}\in\mathfrak{a}^{m_2-e_i}(1\leqslant i\leqslant n)$. 一般地,我们有 $u_{k+1}=u_k-\sum_{i=1}^{n}a_{ki}x_i\in\mathfrak{a}^{m_k+1}M$,$a_{ki}\in\mathfrak{a}^{m_k-e_i}(1\leqslant i\leqslant n)$. 于是对每个 i,$\sum_{k=1}^{\infty}a_{ki}$收敛. 由于 A 完备,从而$\sum_{k=1}^{\infty}a_{ki}=a_i\in A$. 于是对每个 $q\geqslant 0$均有

$$u_1-\sum_{i=1}^{n}a_ix_i=u_1-\sum_{i=1}^{n}\left(\sum_{k=1}^{\infty}a_{ki}\right)x_i=u_1-\sum_{i=1}^{n}\left(\sum_{k=1}^{q}a_{ki}\right)x_i$$

$$-\sum_{i=1}^{n}\left(\sum_{k=q+1}^{\infty}a_{ki}\right)x_i$$

$$=u_{q+1}-\sum_{i=1}^{n}\left(\sum_{k=q+1}^{\infty}a_{ki}\right)x_i\in\mathfrak{a}^qM.$$

由于$\bigcap_{q>0}\mathfrak{a}^q M=(0)$，从而$u_1=\sum_{i=1}^{n}a_i x_i, a_i\in A$，这就证明了$M=Ax_1+\cdots+Ax_n$. ▌

系　设$\mathfrak{a}$为环A的理想，$\bigcap_{n>0}\mathfrak{a}^n=(0)$，$A$对于$\mathfrak{a}$-adic拓扑完备. 如果$G_{\mathfrak{a}}(A)$为Noether环，则$A$为Noether环.

证明　对于A的每个理想$\mathfrak{b}$，$G_{\mathfrak{a}}(\mathfrak{b})=\bigoplus_{n>0}\mathfrak{a}^n\mathfrak{b}/\mathfrak{a}^{n+1}\mathfrak{b}$是$G_{\mathfrak{a}}(A)$的理想，从而$G_{\mathfrak{a}}(\mathfrak{b})$为有限生成$G_{\mathfrak{a}}(A)$-模. 由于$\bigcap_{n>0}\mathfrak{a}^n\mathfrak{b}\subseteq\bigcap_{n>0}\mathfrak{a}^n=(0)$，根据引理25知$\mathfrak{b}$为有限生成$A$-模. 这就表明$A$是Noether环. ▌

定理 9　设$\mathfrak{a}$是环A的理想，$\bigcap_{n>0}\mathfrak{a}^n=(0)$. $\hat{A}$为$\mathfrak{a}$-adic拓扑环A的完备化. 如果A为Noether环，则$\hat{A}$也为Noether环.

证明　由引理4知$G_{\mathfrak{a}}(A)$为Noether环. 再由引理24知$G_{\hat{\mathfrak{a}}}(\hat{A})$为Noether环. 由于$\bigcap_{n>0}\hat{\mathfrak{a}}^n=\bigcap_{n>0}\widehat{\mathfrak{a}^n}=(0)$，而$\hat{A}$对于$\hat{\mathfrak{a}}$-adic拓扑是完备的，从而由引理25的系可知$\hat{A}$为Noether环. ▌

作为完备化的一个应用，我们来证明：正则Noether局部环必为整环. 这首先需要：

引理 26　设$\mathfrak{a}$为环A的理想，$\bigcap_{n>0}\mathfrak{a}^n=(0)$. 如果$G_{\mathfrak{a}}(A)$为整环，则$A$为整环.

证明　设$x,y\in A$，$x\neq 0$，$y\neq 0$. 则$x\in\mathfrak{a}^r-\mathfrak{a}^{r+1}$，$y\in\mathfrak{a}^s-\mathfrak{a}^{s+1}$，$r,s\geqslant 0$. 于是$0\neq\bar{x}\in\mathfrak{a}^r/\mathfrak{a}^{r+1}\subseteq G_{\mathfrak{a}}(A)$，$0\neq\bar{y}\in\mathfrak{a}^s/\mathfrak{a}^{s+1}\subseteq G_{\mathfrak{a}}(A)$.

由于 $G_{\mathfrak{a}}(A)$ 为整环，从而 $0 \neq \overline{x}\overline{y} \in \mathfrak{a}^{r+s}/\mathfrak{a}^{r+s+1}$. 于是 $xy \neq 0$. 即 A 为整环. ▌

系 正则 Noether 局部环 (A, m) 必为整环.

证明 我们有 $\bigcap_{n>0} \mathrm{m}^n = (0)$. 由正则性定义知 $G_{\mathrm{m}}(A)$ 同构于多项式环 $k[t_1, \cdots, t_d]$，$k = A/\mathrm{m}, d = \dim A$. 于是 $G_{\mathrm{m}}(A)$ 为整环，从而 A 也为整环. ▌

注记 本世纪五十年代，采用同调代数方法证明了，每个正则 Noether 局部环均是唯一因子分解整环，这是同调代数在环论中发挥作用的较早例子.

定理 10 设 (A, m) 为 Noether 局部环. 则：A 为正则 Noether 局部环 $\Longleftrightarrow \hat{A}$ 为正则 Noether 局部环.

证明 由于 A 为Noether环，从而 $\hat{A}$ 也是Noether环(定理 9). 由 $\hat{A}/\hat{\mathrm{m}} \cong A/\mathrm{m}$，可知 $\hat{\mathrm{m}}$ 为 $\hat{A}$ 的极大理想. 进而，对每个 $x \in \hat{\mathrm{m}}$，$1-x$ 有逆元素 $1 + x + x^2 + \cdots + x^n + \cdots \in \hat{A}$ (由于 $x^n \in \hat{\mathrm{m}}^n$，可知 $1 + x + \cdots + x^n + \cdots$ 收敛. 并且易证它为 $1-x$ 的逆). 于是 $x \in r(\hat{A})$ ($\hat{A}$ 的大根). 即 $\hat{\mathrm{m}} = r(\hat{A})$. 这表明 $\hat{\mathrm{m}}$ 为 $\hat{A}$ 的唯一极大理想，从而 $\hat{A}$ 为局部环. 由 $A/\mathrm{m}^n \cong \hat{A}/\hat{\mathrm{m}}^n$ 可知 $\chi_{m}(n) = \chi_{\hat{\mathrm{m}}}(n)$. 于是 $\dim A = \dim \hat{A}$. 又因为 $k = A/\mathrm{m} \cong \hat{A}/\hat{\mathrm{m}}$，$G_{\hat{\mathrm{m}}}(\hat{A}) \cong G_{\mathrm{m}}(A)$. 所以：$A$ 正则 $\Longleftrightarrow G_{\mathrm{m}}(A) \cong k[t_1, \cdots, t_d]$，$d = \dim A \Longleftrightarrow G_{\hat{\mathrm{m}}}(\hat{A}) \cong k[t_1 \cdots, t_d], d = \dim \hat{A} \Longleftrightarrow \hat{A}$ 正则. ▌

例 1 设 k 为域，$A = k[x_1, \cdots, x_n], \mathrm{m} = (x_1, \cdots, x_n)$. 则局部环 A_{m} 的完备化为 $\hat{A}_{\mathrm{m}} = k[[x_1, \cdots, x_n]]$(形式幂级数环). 不难看出，$G_{\tilde{\mathrm{m}}}(A_{\mathrm{m}})$ 同构于 $k[t_1, \cdots, t_n], n = \dim A = \dim A_{\mathrm{m}}$. $\tilde{\mathrm{m}} = \mathrm{m}A_{\mathrm{m}}$. 从而仿射空间 k^n 在原点的局部环 A_{m} 为正则 Noether 局部环，而 A_{m} 的完备化 $\hat{A}_{\mathrm{m}} = k[[x_1, \cdots, x_n]]$ 也是正则 Noether 局部

环.

例 2 $A=\mathbf{Z}_{(p)}$表示 $\mathbf{Z}$ 对于素理想 $p\mathbf{Z}$ 的局部化. 于是(A, pA)为 Noether局部环. 以$\hat{A}$表示A对于p-adic 拓扑的完备化, $\hat{A}$叫作是 **p-adic 整数环**. 其中每个元素均唯一表达成 $\alpha=a_0+a_1 p+a_2p^2+\cdots+a_np^n+\cdots$, $0\leqslant a_i\leqslant p-1$. α 叫作是 p-adic 整数. $\hat{A}$是整环,其商域叫 p-adic数域,通常表示成$\mathbf{Q}_p$. 更一般地,设K是代数数域,O是它的代数整数环. 对于O的每个素理想 $\mathfrak{p}$, $O_\mathfrak{p}$是O对于 $\mathfrak{p}$ 的局部化. 以$\hat{O}_\mathfrak{p}$表示 Noether 局部整环 $O_\mathfrak{p}$ 对于 $\mathfrak{p}$-adic 拓扑的完备化(对于 Dedekind 整环O的素理想 $\mathfrak{p}$,显然 $\bigcap\limits_{n>0}\mathfrak{p}^n=(0)$). 整环$\hat{O}_\mathfrak{p}$的商域通常记成$K_\mathfrak{p}$, 叫作是$K$在 $\mathfrak{p}$ 的局部域. 由全体局部域 $K_\mathfrak{p}((0)\neq\mathfrak{p}\in\mathrm{Spec}\,O)$来把握$K$的性质,是代数数论中一种重要的研究手段.

习　　题

1. 求证一维正则 Noether 局部环是离散赋值环.

2. 设A为 Noether环,M为有限生成A-模,$\mathfrak{a}$为A的理想,$\hat{A}$,$\hat{M}$分别是A和M对于$\mathfrak{a}$-adic拓扑的完备化,求证有$\hat{A}$-模自然同构$\hat{M}\cong\hat{A}\otimes_A M$

3. 设A为Noether 环,$\mathfrak{a}$为A的理想,M,N,G均为有限生成A-模. $\hat{A}$, $\hat{M},\hat{N},\hat{G}$ 分别为A,M,N,G对于$\mathfrak{a}$-adic 拓扑的完备化.

(1) 若$f:M\to N$为A-模同态. 求证f是拓扑A-模的连续同态(对于$\mathfrak{a}$-adic 拓扑),特别地,f将M中Cauchy序列(极限为0的序列)映成N中Cauchy序列(极限为 0 序列). 由此自然诱导出$\hat{A}$-模同态$\hat{f}:\hat{M}\to\hat{N}$.

(2) 若$M\xrightarrow{f}N\xrightarrow{g}G$为$A$-模正合序列,求证$\hat{M}\xrightarrow{\hat{f}}\hat{N}\xrightarrow{\hat{g}}\hat{G}$为$\hat{A}$-模正合序列.

(3) 求证$\hat{A}$为平坦A-模.

4. 设$A=\{f:\mathbf{R}\to\mathbf{R}\,|\,f$为无穷次可微实函数$\}$. 在$A$中定义

$$(f\pm g)(x)=f(x)\pm g(x),\quad (fg)(x)=f(x)g(x)\quad (x\in\mathbf{R}).$$

求证:A由此形成环,$\mathfrak{m}=\{f\in A\,|\,f(0)=0\}$是$A$的极大理想,并且 $\bigcap\limits_{n>0}\mathfrak{m}^n\neq$

(0)。

5．设A为 Noether 环，$\mathfrak{a}$为A的理想．求证以下四个命题彼此等价．

(1) $\mathfrak{a}\subseteq r(A)$($A$的大根)；

(2) 每个有限生成A-模对于$\mathfrak{a}$-adic 拓扑均是 Hausdorff空间；

(3) 对每个有限生成A-模M，M的子模对于$\mathfrak{a}$-adic 拓扑均是M的闭集；

(4) A的每个极大理想对于$\mathfrak{a}$-adic拓扑均是A的闭集。

6．A为 Noether 环，$\mathfrak{a}$为A的理想，M为有限生成A-模，M_1，M_2为M的A-子模，$\hat{A}$，$\hat{M}$，$\hat{M}_1$，$\hat{M}_2$分别为它们对$\mathfrak{a}$-adic 拓扑的完备化，求证

(1) $(M_1+M_2)^\wedge=\hat{M}_1+\hat{M}_2$，$(M_1\cap M_2)^\wedge=\hat{M}_1\cap\hat{M}_2$，

$(M_1:M_2)^\wedge=(\hat{M}_1:\hat{M}_2)$。

(2) 设$\mathfrak{b}_1$，$\mathfrak{b}_2$为A的理想．求证$(\mathfrak{b}_1\mathfrak{b}_2)^\wedge=\hat{\mathfrak{b}}_1\hat{\mathfrak{b}}_2$。

7．设A为 Noether 整环，K为A的商域，$A\neq K$．$\mathfrak{a}$为A的理想，$\mathfrak{a}\neq A$．求证A的$\mathfrak{a}$-adic 拓扑与A作为$\mathfrak{a}$-adic拓扑空间K之子空间的诱导拓扑是不一致的，并且A对于后一拓扑不是 Hausdorff 空间。

附录　关于域的扩张

设K和F是两个域. 如果K是F的子域,则称F为K的**扩域**或**扩张**. 这样一对域通常表示成F/K.

设F/K和E/K均是域的扩张. 如果$\varphi: F\to E$是域的单同态(或称作是域的**嵌入**),并且φ在K上的限制$\varphi|_K$是域K的恒等自同构,则称φ是**K-嵌入**. 例如,若1是域F的加法无限阶元素,则$\varphi: \mathbf{Q}\to F, \dfrac{m}{n}\to\dfrac{m\cdot 1}{n\cdot 1}$ $(m,n\in \mathbf{Z}, n\neq 0)$是域的嵌入,即$F$中有子域$\{a\cdot 1|a\in \mathbf{Q}\}$同构于$\mathbf{Q}$. 我们将$\{a\cdot 1|a\in \mathbf{Q}\}$等同于$\mathbf{Q}$,它也是$F$中最小的子域,称作是$F$的**素域**.而这时域$F$叫作**特征为零**. 如果1是$F$中加法有限阶元素,则1的阶必为素数$p$. 这时$F$中最小子域为$p$元域$F_p$. 称$F_p$为$F$的**素域**,而这时域$F$叫作**特征为$p$**. 于是按照1的加法阶特性我们把域分成两大类:特征为零或特征为素数p. 当F的特征为p时,对于任意$\alpha,\beta\in F$, $(\alpha+\beta)^{p^n}=\alpha^{p^n}+\beta^{p^n}$.

现在谈域扩张的分类. 设F/K为域的扩张. F作为域K上向量空间,其维数$\dim_K F$叫作是扩张F/K的**次数**,表示成$[F:K]$. 如果$[F:K]$有限,则称F/K是**有限(次)扩张**. 否则叫**无限(次)扩张**. 利用简单的线性代数知识即可证得:若E/F和F/K均为域的扩张,则$[E:K]=[E:F][F:K]$. 特别地,E/K为有限扩张$\Longleftrightarrow$ E/F和F/K均为有限扩张.

设F/K为域的扩张. 如果存在F的子集S,使得$F=K(S)$(右边表示F中包含$K\cup S$的最小子域),则称F是**S在K上生成的**. 特别若S为有限集,而$F=K(S)=K(\alpha_1,\cdots,\alpha_n)$,则称$F/K$是**有限生成扩张**.又若$S=\{\alpha\}$,而$F=K(\alpha)(\alpha\in F)$,则称$F/K$是**单扩张**. 易知有限扩张一定是有限生成扩张. 但反之不然. (其原因参考下面的(一).)

设F/K为域的扩张,$\alpha\in F$如果存在非零多项式$f(x)\in K[x]$,使得$f(\alpha)=0$,则称α为K上代数元素,或叫**α在K上代数**. 这时,$K[x]$中存在唯一的首一(即最高次项系数为1)多项式$f(x)$,使得:(1) $f(\alpha)=0$, (2) $g(x)\in K[x], g(\alpha)=0\Rightarrow f(x)|g(x)$.称$f(x)$为**$\alpha$在$K$上的极小多项式**.如果$\alpha$在$K$上不是代数元素,即$\alpha$不是$K[x]$中任何非零多项式的根,则称$\alpha$为$K$上的超越元素,或叫**$\alpha$在$K$上超越**. 如果$F$中每个元素在$K$上均是代数的,则称

F/K 为代数扩张. 否则, 即 F 中至少有一个元素在 K 上是超越的, 则称 F/K 为超越扩张. 这两种扩张的最本质区别是

(一) 设 F/K 为域的扩张, $\alpha\in F$.

(1) 若 α 在 K 上代数. 令 $f(x)$ 为 α 在 K 上的极小多项式, $\deg f(x)=n\geqslant 1$, 则 $K[\alpha]=K(\alpha)$ (F 的子域), $1,\alpha,\cdots,\alpha^{n-1}$ 为 K-向量空间 $K(\alpha)$ 的一组基, 从而 $[K(\alpha):K]=n$. $f(x)$ 为多项式环 $K[x]$ 中不可约多项式, 从而 $K[x]/(f(x))$ 为域. 并且有域的自然同构: $K[x]/(f(x))\cong K(\alpha)$, $g(x)\ (\mathrm{mod}\ f(x))\mapsto g(\alpha)$.

(2) 如果 α 在 K 上超越, 则环 $K[\alpha]$ 自然同构于多项式环 $K[x]$, 而域 $K(\alpha)$ 自然同构于有理函数域 $K(x)$, 从而 $K(\alpha)/K$ 为无限扩张 (但这是有限生成扩张).

设 F/K 为域的扩张, $\alpha_1,\cdots,\alpha_n\in F$. 我们称 $\{\alpha_1,\cdots,\alpha_n\}$ **在 K 上是代数相关的**, 是指存在非零多项式 $f(x_1,\cdots,x_n)\in K[x_1,\cdots,x_n]$, 使得 $f(\alpha_1,\cdots,\alpha_n)=0$。反之, 如果不存在非零多项式 $f(x_1,\cdots,x_n)\in K[x_1,\cdots,x_n]$, 使得 $f(\alpha_1,\cdots,\alpha_n)=0$, 则称 $\{\alpha_1,\cdots,\alpha_n\}$ **在 K 上代数无关**. 更一般地, F 的一个子集 S (可能是无限子集) 叫作在 K 上代数无关, 是指 S 的每个非空有限子集均在 K 上代数无关. 可以证明, 若 S 和 T 均是 F 的极大 K-代数无关子集, 则 $|S|=|T|$. 换句话说, F 中所有极大 K-代数无关子集有相同的势数. 这个势数叫作是扩张 **F/K 的超越次数**. 例如设 K 为域, x 为未定元, $F=K(x)$ 为 K 上关于 x 的有理函数域. 不难证明, 对每个 $\alpha\in F-K$, α 在 K 上超越, 并且 $F/K(\alpha)$ 是代数扩张. 于是 $\{\alpha\}$ 为 F 的极大 K-代数无关集合. 从而 $K(x)/K$ 的超越次数为 1. 类似地, $K(x_1,\cdots,x_n)/K$ 的超越次数为 n.

以下着重谈代数扩张. 下面是代数扩张的最基本性质.

(二) (1) 有限扩张必为代数扩张.

(2) 设 F/K 为有限生成扩张, $F=K(\alpha_1,\cdots,\alpha_n)$. 如果 α_i 在 K 上均是代数的 $(1\leqslant i\leqslant n)$, 则 F/K 为有限扩张, 从而也是代数扩张.

(3) 若 E/F, F/K 均是代数扩张, 则 E/K 也是代数扩张.

(4) 设 F/K 为域的扩张, $M=\{\alpha\in F\mid\alpha$ 在 K 上代数$\}$, 则 M 为 F/K 的中间域 (即 M 为域并且 $F\supseteq M\supseteq K$).

(5) 设 K 为任意域, 则存在域 Ω 使得: (a) Ω/K 为代数扩张, (b) $K[x]$

中每个非零多项式$f(x)$在Ω中均有根.(这也等价于说:$f(x)$的全部根均在Ω之中. 或者还可说成,$f(x)$在$\Omega[x]$中分解成一些一次多项式之积.)我们称Ω是K的**代数闭包**. K的任意两个代数闭包都是同构的. 即K的代数闭包本质上只有一个. 如果域K等于它的代数闭包Ω,则称K是**代数封闭域**. 熟知的复数域C是代数封闭域.(注意:C/Q是超越扩张. 例如$e,\pi,\log 2$均在Q上超越,但是Q在C中有唯一的代数闭包.)

(6) 设K为域,Ω为K的一个代数闭包. 对于每个$0\neq f(x)\in K[x]$, $\deg f(x)=n\geqslant 1$. 则$f(x)=a(x-\alpha_1)\cdots(x-\alpha_n)$,$\alpha_1,\cdots,\alpha_n\in\Omega$,$a$为$f$的首项系数. 我们称$K(\alpha_1,\cdots,\alpha_n)$为$f(x)$在$K$上的**分裂域**. 这也是$\Omega/K$的最小中间域,使得$f(x)$在其上可分解成一次多项式之积. 如果$\Omega$和$\Omega'$是$K$的两个代数闭包,$N$和$N'$分别是$\Omega$和$\Omega'$中$f(x)$在$K$上的分裂域,则$N$和$N'$同构. 换句话说,$f(x)\in K[x]$在$K$上的分裂域本质上只有一个.

(7) 设K为域,Ω为K的代数闭包. $f(x)$为$K[x]$中不可约首一多项式,$(x)=(x-\alpha_1)\cdots(x-\alpha_n)$,$n=\deg f\geqslant 1$,$\alpha_i\in\Omega$. 令$\alpha=\alpha_1$. $F=K(\alpha)$. 则对每个$i(1\leqslant i\leqslant n)$均存在唯一的$K$-嵌入$\varphi_i:F\to\Omega$,使得$\varphi_i(\alpha)=\alpha_i$. 并且每个$K$-嵌入$F\to\Omega$均有如此形式. 于是$F$到$\Omega$中的$K$-嵌入个数等于$\alpha$的极小多项式$f(x)$的相异根个数. 元素$\alpha_i$均叫作是$\alpha$的**$K$-共轭元素**.

最后谈域扩张的可分性. 设F为域,$f(x)\in F[x]$,$\deg f\geqslant 1$. 称$f(x)$为F上(或$F[x]$中)**可分多项式**,是指$f(x)$在$F[x]$中的每个不可约因子均没有重根. 例如$f(x)=x^2-2x+1$是Q上的可分多项式. 因为$f(x)$在$Q[x]$中的不可约因子$x-1$没有重根.

可以证明:如果F是特征为零的域,则$F[x]$中每个多项式均是可分的. 而当F的特征为素数p时,对于每个$a\in F$,如果$a\notin F^p=\{b^p|b\in F\}$,则$x^p-a$便是$F[x]$中一个不可分的不可约多项式.

设E/F是域的代数扩张,$\alpha\in E$. 称α**在F上可分**,是指α是$F[x]$中某个可分多项式的根. 这也相当于说α在F上的极小多项式无重根. 如果E中每个元素在F上均可分,则称E/F为**可分扩张**. 可分扩张有如下一些重要性质.

(三) (1) 有限可分扩张必为单扩张.

(2) 设E/F为有限可分扩张,$E=F(\alpha)$. $[E:F]=n$. $f(x)$为α在F上

的极小多项式．则$f(x)=(x-\alpha_1)\cdots(x-\alpha_n)$，$\alpha_i\in\Omega$（$\Omega$为$E$的代数闭包），$\alpha=\alpha_1$。而$\alpha$的$F$-共轭元素$\alpha_i(1\leqslant i\leqslant n)$两两不同。从而恰好有$n$个$F$-嵌入$\varphi_i:E\to\Omega$，其中$\varphi_i(\alpha)=\alpha_i$。

设E/F是域的代数扩张．$\alpha\in E$．称α**在F上纯不可分**，是指α在F上的极小多项式$f(x)$在E的一个代数闭包Ω中只有一个根α。这也相当于说，$f(x)$在$\Omega[x]$中分解成$f(x)=(x-\alpha)^m$，$m=\deg f(x)$。例如：F中每个元素在F上均是纯不可分的（取$m=1$）。又如：令$E=\mathbf{F}_p(t^{1/p})$，$F=\mathbf{F}_p(t)$，则元素$t^{1/p}\in E$在F上的极小多项式为$f(x)=x^p-t$，它只有一个根$t^{1/p}$，（$x^p-t=(x-t^{1/p})^p$）从而$t^{1/p}$在$\mathbf{F}_p(t)$上纯不可分。如果E中每个元素在F上均纯不可分，则称E/F为**纯不可分扩张**。

（四）（1）设E/F为域的代数扩张，令$M=\{\alpha\in E\mid\alpha$在$F$上可分$\}$，则$M$是$E/F$的中间域，并且$M/F$为可分扩张，$E/M$为纯不可分扩张。

（2）设E/F是有限纯不可分扩张。如果$E\neq F$，则E（从而F）的特征必为素数p，并且有$q=p^l(l\geqslant1)$，使得$E^q\subseteq F$。

索　引

七　画

八　画

九 画

十 画

十一 画

十二 画

十三 画

十四 画

十六　画